UNDERCOVER WORK

A Complete Handbook

by Burt Rapp

UNDERCOVER WORK

A Complete Handbook

by Burt Rapp

TABLE OF CONTENTS

Introduction 1
The Undercover World 4
Getting Down to Cases 6
Glossary 20
Starting Up 31
Undercover Work and the Law 37
Recruiting Agents 44
Training the Agent 49
Briefing for the Assignment 55
Establishing Cover 61
Infiltration 68
Roping or Gaining Confidence 76
Employee Theft 81
Working Narcotics 86
Protecting the Informer 91
Undercover Weapons 95
Avoiding Pitfalls in Undercover Operations 100
Controversial Aspects of Undercover Work 105
Blackmail 106
Entrapment: A Post-Graduate Course 111
Industrial Espionage 115
Methods of Payment 120
Planting Evidence 124
Bowing Out: Termination of the Assignment 129
Defensive Measures 132

INTRODUCTION

Undercover operations and their obvious relation to the techniques of espionage, have acquired a mystique and image of glamour that overshadows how truly grimy they often are, and the abuses that can result from them. In reality, an undercover operation is a tool, morally neutral, and it's the people using the tool who make it worthwhile or sleazy. This volume will clear up the misconceptions and attempt to relate how the different facets of undercover operations fit together.

Undercover work of all sorts is, by its very nature, hidden from the public eye. This secrecy often serves the purpose of a "license to kill," a way of implementing immoral and illegal acts without discovery or blame. There's no way of finding out the proportion of undercover work that serves such negative purposes. Apart from a very few practitioners of the art who write their autobiographies at the ends of their careers, undercover agents and their employers keep silent. Obviously, those who have crossed the line into illegal acts have very good reasons for not speaking out. The authors of the autobiographies who have disclosed their stories are, understandably, describing only the deeds which will bring them credit. Selective memory helps them to "forget" any illegal or questionable investigations in which they took part.

There are a few textbooks on undercover operations, dealing with the people and the techniques. These are helpful, but don't begin to give an idea of the proportion of illegal acts committed undercover. Some have veiled references, showing that these practices exist, and some contain warnings against committing illegal acts.

A lot of information regarding undercover work comes by word-of-mouth. Every investigator has his list of informers, and also his little repertoire of tricks and secrets. Some of the investigative techniques would be compromised if they were common knowledge, and others are illegal, which is an even better reason for not documenting them.

Contrary to popular impressions, much undercover work is inefficient and wasteful, and doesn't produce the needed results. This is one aspect that most textbooks don't admit directly. Their authors, investigators themselves, don't want to admit publicly that they spin their wheels so much of the time.

What, then, can the reader gain from *this* book?

First, an understanding of the basic concepts and techniques, both legal and illegal.

Second, an estimate of his own vulnerability to undercover work. Many people who feel they lead honest lives, and therefore have nothing to hide, will be surprised to find there is a corps of undercover investigators who specialize in entrapping people and in "planting" evidence. This need not be in connection with criminal or political cases. Undercover work is common in labor-management conflicts, and unethical and ambitious people use some of these techniques for personal advancement by compromising rivals in the corporate setting.

Third, a grounding in the techniques of security and self-protection.

Fourth, insight into what to expect from undercover work. The reader may have need for it some day, and may be misled into hiring an expensive but ineffective "agency" for this. The agency, if run dishonestly, will try to extract as much money as possible from the customer, needlessly spinning the project out to earn higher fees. Providing "intelligence" that is spurious or alarming is one way to do this, and it's practiced by both private and government agents.

Finally, the reader will learn how to mount an undercover operation of his own, if the need arises. He'll learn how to recruit agents, run them, manage them to gain information and evidence, and how to avoid some of the pitfalls of undercover work. What he lacks in experience, he'll make up in enthusiasm and care, because he'll have the most to gain and the most to lose.

It's a dirty world out there, and the first step to self-protection is to know the defensive tactics, and in severe cases, how to strike back. This book will provide an excellent beginning for both.

THE UNDERCOVER WORLD

There's a remarkable resemblance between international espionage and undercover work by police and private agencies, but here we will concentrate mainly on civilian undercover work. There are several purposes for undercover work as practiced by police and private parties:

(1) *To gain information about criminal activities.* Often, information is enough for the immediate purpose, because it provides leads for further investigation. An example is discovering where a narcotics dealer keeps his "stash." With this information, a police investigator can obtain a search warrant to seize the evidence.

(2) *To gather evidence about criminal activities.* This is a more demanding task, as the evidence must hold up in court and the undercover agent must not taint it by any illegal practice if his testimony will be required.

(3) *Industrial espionage.* This is common practice, much more than the public knows. Since it's a clandestine activity, it doesn't appear in the media unless there's discovery of an agent, and even then it may be handled by other means. "Turning" and "playing back" may be more advisable than prosecution.

(4) *Labor-management disputes.* Both unions and management use spies, sometimes clumsily and quite openly, but mostly undercover.[1]

(5) *Private investigations.* To expose employee disloyalty or dishonesty. This can overlap with industrial espionage, as some industrial spy-masters attempt to recruit employees who can be persuaded to deliver information.

(6) *To entrap.* This is a no-no, but in fact the difference between roping and entrapment is often only the agent's testimony, and in court, the jury's likely to disbelieve the accused, especially if he has a criminal record.

There's also a remarkable similarity between private and police methods of undercover operations. This is because in undercover work, the police can't use their full authority: seeking search warrants, deploying SWAT teams, and other obvious measures. Undercover work is done by stealth, not by force, and it requires a delicate touch. Basically, the police have to follow the same methods as private investigators, since flashing a badge would give away the operation.

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, p. 22.

GETTING DOWN TO CASES

A look at two undercover operations, one run by a police agency and one a strictly unofficial one run by private parties, will show how the nuts and bolts of undercover work relate to real life. This examination will also reveal the uncertainties involved in the secret world, and how what seems to be often doesn't correspond to what really is.

Operation Red-Hot Poker

This was an undercover operation against prostitution, run by a local police agency. It was under the direction of the detective division, but the operation required so much man-power that it drew in people from other divisions.

There were, in this city, a number of houses of prostitution operating under the guise of "massage parlors," "escort services," and "sex therapy clinics." Unlike the streetwalkers, these operations were not out in the open. They were strictly indoor operations, and the prostitutes tried to keep low profiles.

They advertised in sex-oriented newspapers to attract clients. Building a case against them required some undercover and collateral work by the detectives.

The most vital evidence was to be an undercover officer who would be able to testify that the girl made an offer of sex for pay to him. Corroborating evidence was to be rental agreements, showing in whose name the premises were, and telephone company records, showing which numbers were dialed and to whom they were billed. The detectives obtained some of this evidence by trash surveys, rummaging through the trash to find the supporting material.

The trash details were conducted at night by detectives and other officers who first established the trash pick-up days, then went into the alleys and yards the night before, when presumably the dumpsters would be fullest. The collateral evidence collected included condoms, discarded dildoes and other sex toys, telephone bills, notes on clients, appointment books, jars and tubes of sexual lubricants, and other items which served to provide information or evidence.

While possession and use of sex toys, lubricants, and the like are not in themselves illegal, the volume gathered served to build up a picture of a systematic operation on the premises. Finding fifty used condoms in the trash of an apartment supposedly housing one married couple suggests there is more going on than the customary sex relations, no matter how sexually active the couple might be.

The vital evidential component, however, remained the offer of sex for pay, or solicitation. For this undercover officers were essential.

The cover required was hasty and superficial, the only "must" being that they not appear to be police agents. The detectives chosen for these roles had to pass as ordinary citizens, with physical appearances not suggesting the police.

There's a certain physical type that police seem to prefer. This is the young, healthy, clean-cut athletic

type, and this image would serve as a give-away. The detectives in the undercover unit mostly did not fit this pattern, tending to be sloppy, overweight, and over-age. They did seem plausible clients for these services.

There were some complications. One of the requirements of building a case was that the offer had to come from the prostitute, to avoid any suggestion of entrapment. The undercover officer would have to telephone the number listed in the newspaper ad and request "service." The prostitute would not discuss sex acts or prices on the phone, and required a personal meeting. This met the officer's need, because to have a case he had to identify the voice with the prostitute, difficult to do without a face-to-face meeting.

At the meeting, the officer had to let the prostitute mention the price. He could, under the guidelines laid down by the public defender's office, tell the prostitute exactly what he wanted, but could not himself suggest that she do it for pay, to avoid any taint of entrapment. Once the officer got the offer, he would have to leave. This was because the policy clearly stated that the officers could not actually engage in sex acts.

Statute and case law limit an officer's involvement in a crime. Excessive participation can constitute entrapment. This is a murky subject, and many agencies "play it safe" to avoid crossing the thin line and compromising the case.

There's also a personal element in vice operations. In sex investigations, it can intrude significantly, because many of the officers are married. If they were to tell their wives what their jobs entailed, and if it required having sex with the prostitutes, some of the wives would surely object, protesting that their husbands were getting to like their jobs too much. Normally, some wives do object to their husbands'

assignments to vice, because they have dark suspicions regarding what the work involves.

We see the same problem in narcotics investigations, which involve a lot of undercover work. The undercover agent may make a "buy," but requiring him to become an addict is simply asking too much.

This points up some of the limitations in undercover work, and shows why it's often easier to "turn" someone who is already criminally involved than to have an officer assume the role.

In "Operation Red-Hot Poker," it was required that two officers separately work each house of prostitution, in order to have mutually supporting evidence for the search warrant affidavits. This brought up another problem. The officers had to make up excuses to leave. Some of them claimed attacks of conscience, and a reluctance to cheat on their wives. Others claimed a last-minute fear of venereal disease. All of these excuses seemed plausible, but the intense investigation formed a pattern, and the detectives were concerned that the sudden increase in "dry runs" would arouse the suspicion of the prostitutes.

There was a way around this. Although the officers were enjoined from going through the sex act with their targets, there was no rule applying to civilian volunteers. Accordingly, some were recruited and provided with the money to pay, and instructed to go through with sex with the girls.

Once all the evidence was in hand, the detectives made out affidavits for the search warrants, and raided the premises, scooping up the prostitutes, their sex toys, lubricants, and pornographic magazines, and most importantly, their "John files," or "trick lists." The fact that the trick lists had been seized was widely publicized, although the lists themselves were not published. This was a collateral

effort to deter potential clients through the knowledge that if they patronized prostitutes, their identities would be on file and open to seizure by the police.

At least, this was the assumption under which the police supposedly labored. This was naive. It's hard to imagine anyone giving his real name to a prostitute. Possibly some did, but it's more likely that they gave assumed names, and even identities taken from the telephone directory. There was no wholesale prosecution of clients in the aftermath of the operation, which suggests very strongly that most of the names were fictitous.

Let's move on to another case, which was much more complicated because it was entirely unofficial, and thus was not subject to any legal restrictions.

Operation Union

In one workplace, the employees were intensely dissatisfied with working conditions, and one of them solicited the representation of a labor union. The local's president came to the shop, and visited the employees at home, to ask them to sign National Labor Relations Board cards requesting a certification election. This election would be to determine if a union would represent them in collective bargaining. The following is a first-person account by one of the employees who became a central figure in the action. It's unedited, to give the full flavor of the case:

When Mel, the union president, came around, I was lukewarm to the idea. I thought that a union might not be able to do much for us, and that a lot of it would be wasted effort. We had a good production manager who was doing his best for us. Still, I signed up because I thought it might be worth trying. I found out that this turned into a really dirty and nasty fight, and resulted in a disaster for almost everybody in the shop.

First, the union did manage to sign up the majority needed to hold an election. The company executives then tried to sweet-talk us into sticking with the company and rejecting the union. They were very nice to us, took us out to breakfast, gave nice speeches, and generally sucked up to us. We found out, though, that behind those words was a lot of hate and resentment.

One thing that they did was use spies. These were their ass-kissers. These people kept their ears open to find out who was pro-union, and reported back to the bosses. They attended union meetings, to see who else was there. The union president told me he knew every company had spies, and the company president got a report on each meeting as soon as it was over.

We both knew this was illegal, but knowing it and proving it are two different things. The union president felt he couldn't do a thing. Also, he was against violence, as I was, and didn't approve of actions such as slashing their tires. I knew some unions did things like this, and they got what they wanted, and in a way regretted that we were so clean. Maybe it was all for the best, but in the following months I had a lot of reason to doubt this kid-glove policy.

A little before this happened, Johnny Patrick came to work there. He was a nice little guy, always ready with a smile, and a very friendly

manner. He said he'd been a Marine in Vietnam, and that he'd done some "soldier of fortune" work since. I found him interesting, and we became friends. When the union thing came up, we wound up on opposite sides of the fence, but we didn't let this ruin our friendship. He was a solid company man, and didn't pretend to be otherwise. Still, we went out drinking together, and did some crazy things.

I wondered about him, though. Though we were on opposite sides, I never tried to pump him about the other side, even though I knew he was in solid with management. I suspected that he kept up his friendship with me because he thought he might influence me, or pump me. He really did try to get me to change my mind a couple of times, while we were drinking.

Because the ass-kissers always came to union meetings, those of us who were most for the union formed a core group. We met informally, between the open meetings, because we had things to discuss that we didn't want reported back to the bosses by the spies.

What brought me out solidly on the side of the union was a comic book the company artist drew against the union. When I saw that, I hit the roof. It was an insult to our intelligence that the management felt they had to produce propaganda in comic-book form to convince us. From that point on, I was a union man, 100%.

Bit by bit, we did our work among the people who were still lukewarm. As it went, it was very close. A lot of people were afraid for their jobs, because rumors were going around that everybody connected with the union would be fired, or that the owners would sell the company if the union won.

The union won by one vote. During the election, the NLRB had appointed three people from the

company side and three from the union to sit as observers. I was one of the observers. I saw a woman, who'd been pro-company and yet attended union meetings, taking notes. Under the rules, a copy of which I had, it's illegal to record who votes in a certification election. I asked the NLRB representative, who was conducting the election, if the rules meant what they said. She answered yes, and I asked the woman to show us what she was writing down. She brought the paper up to me, and it was a list of people who'd voted so far. I showed this to the NLRB rep, and that was the end of it.

After the votes were counted, I saw a funny thing. Johnny Patrick went up to the company president in the lobby and said to him: "You'll have my resignation on your desk Monday morning." I thought that was odd, and had my suspicions why he said that. I was never able to prove it, though. I never asked Johnny, because I felt he'd never give me a straight answer, anyway.

One month later, the owners sold the company. The union had to negotiate a contract with the new owners, and just setting up meetings took a lot of time. I'd been shop steward, and then we had an election for shop steward, and another guy won.

The new owners also had another company in the same line of work, and they decided to combine the two. We realized this would make the union members outnumbered, and weaken our position. This was a worry, because we were starting to suspect the new owners would not negotiate in good faith, no matter what the law said. It looked as if they were stonewalling the negotiations already.

Shortly after taking over, they started layoffs. One day, they laid off a whole shift, which by coincidence was the shift that was all union men,

and we thought that was dirty pool. One of the people laid off was the shop steward, and the president of the union appointed me again.

It was about this time I thought we'd better get some solid information about the new owners' intentions. I felt my responsibility as shop steward very heavily, and thought I'd better try to do what I could. I decided to do a little spying, without telling anyone, not even the union president.

I had some friends in the front office, closer to the executive suite than I was. I decided I would try to get some information from them. One of them was the comptroller, a very decent guy who had no respect for the new management because one of the people they'd laid off, the production manager, was a good friend of his.

I arranged to meet him after hours. I paid for the drinks and supper, and told him right out that I needed information. He was glad to help out. He told me the new owners had no intention of signing a contract with the union, and intended to delay it as long as they could, meanwhile finding one reason or another to lay people off, and also wait for others to quit, so that in a year they could hold a decertification election with the NLRB and win. They already had the votes by bringing in their employees from the other plant.

We met several times, always after work, and always at a place far enough from the shop that nobody would see us together, except by very bad luck. We watched to see if we were being followed, but never saw anything suspicious. We both knew he was laying his job on the line by providing me with information, and I wanted to protect him. The union hadn't protected many people so far, and I didn't want to make it worse.

I promised him I would keep his identity secret, because I felt I owed it to him, and I kept that promise, even though it cost me later.

I wanted as much information as I could get, just to make sure. Another guy I tapped was in the sales department, a youngster who was very decent, and resented what was going on, even though it didn't affect him personally. I met with him after work, and he told me basically the same thing.

A third guy I tapped was a sales manager. He confirmed what the others said. None of these guys knew I was asking the others. I felt that if these people were risking their jobs, I should do my best to protect them by keeping their involvement secret, even from each other. I could never be sure that one wasn't a company fink. I also wanted each to think he was alone in feeding me information, in case he was trying to tell me a story.

What impressed me was that all three agreed, independently. Once I had the picture, I went to the union president.

This was a disaster. He just wouldn't take me seriously. I couldn't tell him exactly who my sources were, and I felt this weakened my case. Later, I realized maybe he was holding my friendship with Johnny Patrick against me, as everyone knew that Johnny was a 100% company man. Maybe it was simply guilt by association, and nobody trusted me anymore.

Looking back, I know my information was right, although it might not have looked solid at the time. The union never got a contract, and some months after that even the solid union people gave up hope and started leaving. I left around that time. A year later the company folded.

Looking at these two case histories, we can see some similarities and some significant differences.

In both instances, there was a need to preserve secrecy. The police didn't want to blow the operation, and the shop steward wanted to protect his sources. With the police, the undercover roles had only to last a few minutes, long enough to obtain a solicitation from the prostitutes. In and out. In the second case, it was necessary to preserve secrecy for much longer, and for two reasons: to maintain the sources, and to protect them from reprisals by management. If they'd been fired, they would no longer have been able to report information. Personally, they would have suffered the consequences of what management would have considered betrayal. This might well have followed them through their careers, poisoning their references.

In both instances, meeting places were apart from the target premises. The detectives met with their undercover men out in the field, or at the office, without risking compromising them. The shop steward had to be very careful in arranging meetings. He made sure that he wasn't tailed when he went to a meeting, and never saw any indication of a tail. This isn't surprising, because the issue simply didn't justify that level of effort from management.

The police had the law on their side, and could make it stick, if they followed the proper procedures. Although the police complain vehemently about being hamstrung by legal technicalities, they can get search warrants, and they can bring a case to court.

Both the company and union were operating without the sanction of law. The law as it's written and as it's enforced are not necessarily the same thing. The shop steward had no power to obtain a search warrant or any of the advantages the police have. He had to do it all totally undercover and alone.

The police have expense accounts. The shop steward had to pay expenses himself. While the police prefer not to pay undercover people and informers, the shop steward had no choice. He could only afford dinners and drinks. He was forced to run a shoestring operation, but this turned out to be no handicap.

The shop steward got good information because he had high-grade agents in place. Johnny Patrick might have been a paid company undercover man, but if he was, he blew it, because he was too talkative. The company might have infiltrated undercover agents that remained undetected, but there's no way of knowing that now.

The police worked two undercover men for each operation they raided, and the shop steward didn't rely on just one source. He had three, and part of his reason for keeping their identities and existence secret was to be able to cross-check, in case one of them slipped him some bad information. This isn't necessarily distrust; it's just a normal security procedure, very much like a spare tire.

His three agents had one thing in common: attitude. Although not one was strongly pro-union, all despised management. They were ideological informers, the best kind.

Another significant aspect was that neither the police nor the shop steward used deep penetration agents. For the police, superficial cover was enough. For the shop steward, his agents were already there, with their jobs as legitimate cover. Thus we can't consider either of these operations intense undercover work, with the laborious building of false identities and cover stories.

Throughout both operations, there was little risk of violence as a result of the intelligence-gathering. Prostitutes normally don't offer armed resistance to arrest, and this union had a history of non-violence.

Although there are other unions that do practice violence as a matter of normal procedure, and informers may wind up floating face-down in the river, no violence occurred in this case. There were no detectable uses of agent-provocaters in the union case history, although this had happened in other companies.

There was also no entrapment in the case of "Operation Red-Hot Poker," and the reason is not hard to understand. Entrapment is often a part of undercover law enforcement,[1] with police officers offering perjured testimony in court, but in this case it wasn't used because it wasn't necessary. The prostitution operations were real, and there was no need to "frame" the arrestees.

Finally, we come to the use of undercover information. The police, well-organized and experienced at making cases, had a 100% success rate, and obtained convictions or guilty pleas from all the people arrested.

The union undercover effort, although skillfully managed with far fewer resources, produced accurate information but failed in the last step: utilization. The person to whom the information was most important, and who had the power to do something with it, brushed it aside for reasons that are still not clear.

These two case histories have covered undercover work as it really is, not textbook examples. They've shown the problems and pitfalls that impede success, what went wrong and what went right.

There are three steps in the handling of information: *Procuring* information, *Evaluating* it, and *Disseminating* the information.

The exact means differ somewhat from case to case. In the case of the police, the undercover agents played somewhat different roles, their information

was straightforward and resulted in search warrant affidavits.

In the case of the union, the acquisition of the information took much longer, the evaluation was more delicate, and proper utilization was more involved than presenting an affidavit to a judge.

We can see that undercover work, like any information-gathering, is one link in a chain. The chain must be intact to serve the purpose. One broken or weak link nullifies the whole effort. This is the principle of grand strategy that rules the game.

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publishers, 1975, p. 70.

GLOSSARY

Between inaccurate factual accounts, and romanticized fictional ones, there's been much confusion over undercover methods and terminology. It will help if we start by defining some of the terms. Many relate both to undercover work and espionage, and some are emotionally loaded. We'll find that many of the terms are synonymous, and that others overlap. We'll also see that people use one term if they approve of the activity, and another if they don't. A basic glossary of undercover work and espionage follows:

AGENT. Anyone who serves a secret purpose. This is a very broad term, and an agent may be a spy, traitor, dupe or another type.

AGENT-IN-PLACE. This is an agent who is already in the target group. He may be a citizen of another country, a member of a criminal gang, or an employee or union member. An agent in place is extremely desirable, because there's no need to build up a cover for him and to take the laborious and sometimes dangerous steps needed to infiltrate him. He already has his cover, and it's 100% legitimate. His job is to provide information, while staying in his position. He has to be careful not to risk exposure,

and there are several methods to reduce the risk, such as using "cut-outs" and "dead drops."

AGENT-PROVOCATEUR. This term comes from the French, and today it's often spelled "agent-provocater," an English adaptation. The agent-provocater's job is to entrap, to "set up" people, by inciting them to commit a compromising act or one for which they can be prosecuted.

A repressive government may try to eliminate an opposition party by prosecuting its members for overt criminal activities, such as attempting an assassination. The Director of the secret police may infiltrate an agent to incite such an attempt and to inform him when it's about to take place, so he can arrest the conspirators and discredit the group.

An agent-provocater may be used as a "loyalty test," an attempt to induce people normally not under suspicion to make disloyal statements. This happens both with governments and in corporations.

A businessman, resenting the presence of a union, may send in an agent to incite union members into something illegal, such as a sit-down strike, violent demonstration, or other action which enables the company to get a court order and the assistance of the police.

BACKGROUND CHECK. This is sometimes called "vetting," and means investigation of a person's background as a preliminary to employment or granting a security clearance. This means interviewing the candidate's friends, former employers and associates, to verify his identity, reliability, and political sympathies. In police practice, a background check also covers criminal records. In private corporate practices, it may also mean checking on possible union affiliations, although this is illegal.

BACKSTOPPING. One of the essentials for deep cover. False documents can provide superficial protection, but they're vulnerable to a background check, and even a casual investigation. A driver's license, no matter how carefully forged, won't survive a check with the motor vehicle office when it turns out there is no such person on file. Similarly, a forged diploma has no school records to back it up.

Backstopping can be quite elaborate, and can require the cooperation of many persons and the insertion of corroborating data into many records. This is relatively easy in one's own country, or one's own company, where cooperation is relatively easy to obtain. It's almost impossible in a foreign country, where there isn't easy access to records.

BLOW. To expose an agent or secret operation, inadvertently, through carelessness or accident.

BURN. To expose an agent or secret operation purposely, or by serious negligence. A police officer who "burns" an informant generally makes it difficult for any other prospect to trust him, especially because burning a source can result in serious violence to that source.

CONTACT. The agent's contact may also be known as his "control." He services the agent, gives him instructions, money and other supplies, and receives information from him. This may be by personal meeting or other means.

COUNTER-ESPIONAGE. An effort to counter another party's espionage. This can include penetrating the opposition's intelligence agency, "turning" his discovered agents, and "playing them back."

COUNTER-INTELLIGENCE. An effort to deny another party's gathering intelligence. This can be through security measures, such as need-to-know, physical safeguarding of documents, or physical barriers such as fences and locks.

CUT-OUT. Similar to a contact. This is to protect the spy-master, or resident, in case the agent becomes compromised and subject to coercion by the opposition. The spymaster often uses a contact or cut-out to service the agent. The cut-out has only the information he needs to do his job, which limits the damage if he's caught and made to talk.

COURIER. This person transmits messages and information. He may, in the case of a verbal message, know the information, but in the case of a coded or written message may not. He differs from the "contact" because he has no authority over the agent. Like the "cut-out," he knows only what he needs to do his job.

COVER. This is the fictional background that a spy or undercover agent obtains to explain his presence. It can be very elaborate, such as when it's necessary to send an agent into a foreign country and provide him with the language skills and paperwork to enable him to pass as a citizen of that country. A police officer may build up a "cover," including false drivers license and other ID, to enable him to pass as someone else in order to infiltrate a criminal gang. A lower level of cover is necessary when a company hires an agent to join the work force to discover employee theft. Then, it's merely necessary to develop a skill in the work, and to pass as a member of the community. This can involve false ID, but often it isn't necessary. In some cases, the cover is very thin, or even unnecessary, as when a member of a

criminal gang or an employee is recruited to serve as an agent. Then, it's only necessary to hide his connection with the police. This is an "agent-in-place."

COVERT. Secret and under cover. A "covert agent" is a secret agent. A "covert resident" is one who disguises his true function, and who may not be in the same country or the same company. A "covert source" is a clandestine source, such as a spy, a stolen document, or a code-breaking operation. Antonym of the term "Overt."

DEAD DROP. A place to leave messages, information, or supplies. This is usually an inconspicuous spot, a hiding place where it's safe to leave material without risk of discovery. The purpose is to avoid contact between the two parties, so that one may not be coerced into identifying the other if caught.

DEEP COVER. A total suppression of true identity and assumption of a false one. Used most often in international espionage.

DEFECTOR. Someone who openly leaves the target group, bringing with him information. A defector is valuable for political propaganda, and the information he brings with him may be quite valuable, but once he defects, he has no further access to information. This is why spymasters usually prefer an agent in place, who may keep feeding them information for years. This type is called a "defector-in-place."

Once a defector has come across, he can expect an intense "debriefing," to extract from him as much information as possible while his memory is still fresh and before the information is out of date. The effects of a defection can be severe for the side from

which he defected, including a tightening up of security, organizational and procedural changes to nullify the information passed, and even arrests and executions.

The defector serves a propaganda purpose, if he's at all political. A citizen of another country, or a member of an opposition party, can come out in the open and renounce his past affiliation. He can state his reasons for so doing, claiming the leaders of the group are tyrannical and immoral, and otherwise defame them. What he doesn't say is as important as his public statements. He may have some less honorable motives for defecting, such as being in trouble with the leaders, or he may be defecting for money and the promise of a good life.

DEFECTOR-IN-PLACE. A synonym for an "agent-in-place." The defector changes loyalty, but remains where he is to pass information. A difference is that the defector changed out of ideology, while the agent may have other motives for serving, such as money or an effort to avoid prosecution. A member of a theft ring who is caught by the police can be "turned" into an agent-in-place, providing information that he would not normally furnish.

DOUBLE AGENT. One who pretends to work for one side while really working for the other. A double agent can come about because he's been caught and "turned," and finds the prospect of betraying his former loyalty more attractive than the consequences if he doesn't. He can also start out as a double agent, seeking to penetrate the opposition's espionage agency while reporting back to his original employer. This can work in a variety of situations. A well-organized gang can, for example, adopt this practice when an agent or informer is discovered. The reasoning is that if they eliminate

the agent, another agent will take his place sooner or later. The next agent may be harder to discover, and the safe course is to nurse the discovered agent along, feeding him false information or even actively recruiting him as a double agent.

ESPIONAGE. This word, from the French, means gathering information by means of spies. The meaning has expanded somewhat in recent years to take in other means such as electronic eavesdropping.

ENTRAPMENT. Provoking another to commit a crime. This is what an agent-provocater does. The agent becomes not only a willing participant in an illegal act, but he incites it. This is illegal in this country, although not in some others.

FREEDOM FIGHTER. An emotionally positive term for anyone who uses violence. See "Terrorist."

INFILTRATOR. See "Penetration agent."

INFORMANT. This is a person, uninvolved with a crime except as a witness, who provides information to the police. An informant is not, in principle, a secret informant. As a bystander, he can openly provide a description of a criminal, and later serve as a witness in a trial.

INFORMER. An undercover agent in place, who provides information for pay or other motives. Police use "informers" a lot, and these informers are usually criminals themselves. They may inform for pay, or to get a "deal" from the police if they've been caught in a crime. An "informer" always works in secret.

This is because he must retain the confidence of the people on whom he's informing, and because of the danger of retaliation. A criminal gang sometimes kills a "squealer." In any case, exposing the informer's connections will "blow" him and end his usefulness. Police often use this term interchangeably with "informant."

INTELLIGENCE. This is a fancy term for information, gathered from open or secret sources. Today, most intelligence comes from open sources. It's unfortunate that the English language uses the word "intelligence" as a synonym for "information," because it carries a connotation of intellectual brilliance, whereas this is often not the case. Other languages are more straightforward. In German, the term is *nachrichten*, or information. In French, it's *renseignement*, again meaning information. This term leads to other abuses. We hear of "intelligence sources," which can be anything from a newspaper account to an informer, and there's a danger in accepting such information uncritically, because it can be wrong, depending on the quality of the source and the interpretation of the person controlling the source.

LEAK. A disclosure of information, for political or criminal purposes. It can be a purposeful leak, as when a politician discloses secret information to help get him re-elected, or it can be otherwise, as when an agent takes it. Security measures are aimed at minimizing or eliminating leaks as well as purposeful espionage.

LIVE DROP. This is a person whom the agent meets to hand over his information.

MAIL DROP. A form of dead drop, in the sense that there's no contact between the agent and the receiver. This may be a commercial mail drop[1] or the address of a private person. It may be a post-office box. The purpose is to avoid the agent's knowing the address of the spymaster.

NEED-TO-KNOW. Restricting secret information to those who have a legitimate use for it. This minimizes the number with access to it, and thus reduces the risk of a "leak."

OVERT. Above-ground, and not secret. This term applies to information gathered from public sources, such as newspapers, press releases, and company literature. It also applies to personnel who operate openly, such as diplomats, police patrolmen and detectives, and company guards.

PENETRATION AGENT. An infiltrator. This type of agent is not part of the target group, and it's necessary to insinuate him into it. This task can be easy, as when hiring an undercover agent to seek out dishonest employees, or it can be so difficult as to be almost impossible, as in trying to place an agent as a member of a foreign country's secret police. Typically, undercover agents are penetration agents, outsiders who "penetrate" into the target group. When an agent is recruited from within the group, he's known as an "informer" or an "informant."

RESIDENT AGENT. This is a term often used for the spy-master, the one who controls a network of agents. The resident may be out in the open, as when he has diplomatic immunity, or when he's the "Director of Security" in a company. His being out in the open does not necessarily compromise his work. He can also be under a sort of cover himself, not

announcing his presence yet taking no risks and not being above-board regarding his true role. In a company, he may have a title such as "Director of Research," "Vice-President in Charge of Special Projects," or another which doesn't disclose his true function.

PLAYING BACK. This is feeding a discovered agent false information to mislead his employer. This not only neutralizes his effectiveness, but enables an active and aggressive operation against the enemy. Playing back goes one step beyond "turning." A terrorist group that discovers a government agent may play him back by feeding him information that they're going to carry out a raid at one location, while they really plan to hit another. This draws government security forces away from the true site and leaves it unprotected. It's also possible to feed back information to lead the opposition to believe that another one of their informers is unreliable. This is a way of neutralizing an informer. Playing back a double agent can become very complex. One side can use him to cast doubt on the reliability of some of the other's personnel, even highly-placed ones. The technique is to feed him information that data has been obtained which could have come only from the target, which will cause him to come under suspicion. Another complication is that the double agent may change loyalties again, making him a triple agent.

ROPING. Gaining the confidence of the group the agent is infiltrating. This requires good cover, discretion, and interpersonal skill, as well as acting ability. The agent must convince the target group that he's one of them. There's a thin line between roping and entrapment, and some agents cross it.

SECURITY. A part of counter-intelligence. This involves passive measures, such as guards and gates.

SNITCH. A slang term for "Informer."

TERRORIST. Someone who uses conspicuous violence. This can be an assassination, planting a bomb or other form of sabotage, or hijacking an aircraft. This is an emotionally loaded term, and whether we call a particular person a "terrorist" or a "freedom fighter" depends on which side of the political fence we stand.

TURN. To "turn" someone is to force or persuade him to change loyalties.

TWIST. A means of coercion. A police officer who offers to drop charges in return for information has a "twist" on his informer. An employer who catches an employee stealing, and makes him a similar offer is using a "twist."

VETTING. See "Background check."

Sources

1. *Directory of Mail Drops in the United States and Canada*, Michael Hoy, Port Townsend, WA, Loompanics Unlimited, 1985.

STARTING UP

An undercover operation can start as a private or company effort, or through a private investigation agency. Private agencies try, by extreme secrecy, to build up a mystique and give the impression they have almost superhuman expertise in clandestine work. This impression is false. There's nothing they can do that a dedicated and intelligent individual can't do for himself.

This requires clarification, because many will disagree. Private investigative agencies are often staffed by retired police officers, who have built up a network of contacts in the law enforcement and criminal worlds. This gives them access to information sources denied to most private citizens. A retired policeman can tap his friends still in active service and obtain a person's criminal history, if any. This is usually illegal, but it's common practice because it's easy to avoid detection. In the states in which access to motor vehicle information is restricted to official agencies, a retired cop can obtain these, too. His network of criminal informers sometimes can be useful in an investigation involving a theft ring.

These advantages aren't absolute. A private individual who's resourceful can work his way around them and obtain the information he needs by other means.

A corporate president, for example, will usually avoid hiring an outside agency, because of the expense. Instead, he'll hire a "director of security" who often is a retired cop, with all the benefits that entails. It's also not commonly known that in many states, drivers license records and vehicle registrations are public information. These are available to anyone who pays the nominal fees.[1]

There's an additional advantage that a private individual has over the investigative agency. The agency is licensed, and under the scrutiny of the state licensing board. This limits its realm of action somewhat. Among other things, state law usually dictates that a private investigator have a clean criminal record, as must anyone working for him. Circumventing this is a risk, and the licensed investigator must be prepared to take a risk if employing a criminal is the only choice he has.

In the real world, unlike the world of public relations brochures, the agency's real function is to convince the client that it's doing a good job, a better one than he could do for himself. Often, the client is intimidated because of his unfamiliarity with the world of private investigation, and spends more than he needs to.

This is the seamy side of private investigative work. The profit motive is often behind some unethical practices. One facet is that private agencies often try to hire the cheapest help they can, and have to settle for the lowest slice of the labor pool. This is why so many "rent-a-cops" are poor quality. Many of their plain-clothes counterparts are no better. While there are retired policemen in the field, there are also failed cops, those who didn't make the grade for one reason or another, or were forced to resign because of questionable or poor performance.

Regarding unethical practices, some employees of private agencies will go overboard in their zeal,[2] and

the result can be quite destructive. To be fair, it's not always the agency's exclusive fault. Some clients solicit illegal actions, or try to make the investigator an inadvertent co-conspirator in a crime. A client might employ an investigator to tail someone on the pretext that he suspects him of an illicit liaison with his wife. Actually, he might be trying to find out his schedule, to set him up for a "hit."

Infiltrating an undercover agent is a lengthy task, and requires a lot of patience and money. However, it's in the agency's interest to spin the case out as long as possible, in order to collect a bigger fee.

These considerations lead to suspicion of any investigative agency, except one recommended by someone whose judgement you respect. Otherwise, you might be burned. You might consider doing it yourself. This isn't as shaky an idea as it might seem at first, because in fact many of the people employed by investigative agencies are of such poor quality that you can probably recruit better yourself. One such agency recruited people who literally walked in "off the street," with no qualifications whatever, to be undercover shoppers. It was a low-grade task, but it's possible that some agents might have fudged their reports in an effort to score points.

There's much to recommend a do-it-yourself operation.[3] Cost is one factor. This should be secondary, but often, with higher executives watching the budget, it becomes critical. An in-house agent costs far less. The outside agent collects his agency salary, the agency tacks overhead and a profit margin onto it, and the agent also collects one from your company.

Even the police have their own in-house security. The New York Police Department, for example, has the most-publicized program of all. It has an office which, whatever the current name, handles "internal affairs." It recruits police trainees while they're still

in the academy, arranging for them to report clandestinely to a member of this secret office. The police-officer-undercover-agent observes his fellow students, and when he graduates, reports on the personnel and events at his patrol assignment. The office uses these "field associates" to uncover evidence of corruption and malfeasance among members of the department.

This measure is necessary because of the closed society that makes up the policeman's world. The rule is: "You don't tell on another cop." This conspiracy of silence has honest officers disapproving of corrupt practices, but keeping silent about them for fear of being ostracized on the job. To overcome this, it's necessary to recruit undercover "field associates" before they become indoctrinated into the cop's world and its clannish values.

A similar, but weaker, ethic permeates both white and blue-collar workers. Among blue-collar employees, there's a strong feeling of "us and them." This leads them to stand together against management, and to turn a blind eye on fellow employees who misbehave. This is part of the "unwritten law."

Among white-collar employees, there's more of an attitude of calculation. The white-collar type is more likely to consider whether disclosure of a fellow employee's dishonesty will help or hinder his career. The dishonest employee might have a friend "higher-up," or may be the visible part of a ring that includes some top executives who could hurt the whistle-blower. On the other hand, it might pay to score some points and establish bonafides, proving company loyalty by snitching on someone dishonest. It can go either way.

Many of the largest corporations have their own security departments, which handle the guard force,

overt investigations, and undercover work. General Motors had 4,200 security personnel in 1978, according to one source.[4]

If you're considering running an undercover operation yourself, you'll find that you have to have a natural flair for it. Someone you hire for this purpose should have similar qualities. The needed skills are, among others:

(1) *The ability to blend in with almost any group.* Someone who feels comfortable in dealing with people will have an easier time of it than someone who is awkward.

(2) *A strong stomach.* You may see things you don't like, but must be able to take them with outward calm.

(3) *Acting ability,* to be able to play a role.

(4) *A good memory,* not only for your cover story, but for the names, faces, and facts you'll encounter and have to remember.

(5) The ability to think on your feet. Improvisation is sometimes vital to working an undercover assignment.

(6) *Alertness.* It's necessary to keep alert to small details, as well as grasp the major events.

(7) Finally, *the ability to avoid romanticizing the task.* There's no room for "James Bond" types here. A starry-eyed romanticist may not be able to overcome the temptation to talk about it, which is extremely undesirable. He also may show excessive zeal, try too hard, and compromise the whole effort.

Formal education isn't vital, unless the assignment requires talent for work that entails a degree. Common sense is the most important quality, because it brings with it the ability to improvise. Last but not least, the quality we call "native intelligence" is important.

Sources

1. *How To Get Anything On Anybody*, Lee Lapin, Auburn Wolf Publishing, 584 Castro Street, Suite 301, San Francisco, CA 94114. Chapter 30, pp. 156-176, tells how to obtain public information such as driving records and vehicle registrations. Included is a list of state offices to contact. This book's a gold mine for anyone wanting to get into the field, although it dwells heavily on technical means, (bugging) and some of the detailed discussions of bugging may be tiresome as well as more than you need.

2. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, p. 16. Barefoot points out that undercover operators do try to entrap innocent people in order to better their positions, and that polygraph tests serve to discover these.

3. *Ibid.*, pp. 9-11. Here, we find a good discussion of the author's experiences at in-house corporate security, and his reasons for preferring such to hiring an outside agency. He makes a good case.

4. *The Private Sector*, George O'Toole, New York, W. W. Norton Company, 1978, p. 42.

UNDERCOVER WORK AND THE LAW

If you're a privately employed undercover agent, you need a basic knowledge of what you're legally empowered to do. Equally important is knowing what you can't legally do. It would be naive to expect that all undercover agents will walk the straight and narrow by respecting the law, but at least this chapter will give you an understanding of what you're facing.

What follows is an approximation of the laws in most of the 50 states. The emphasis here will be "practical," rather than "legal." There's a great difference between how the law reads, and how it's enforced. The main determinant in a civil and criminal action is not guilt or innocence, but vulnerability to prosecution. In plain language, some cases are harder to prove than others. Some law-breakers cover their tracks better than others. This is important to keep in mind because part of your task will be gathering evidence to support prosecution, and the better the evidence you collect, the more successful you'll be.

All of the following will be in plain language, at a slight risk of inaccuracy for the sake of clarity. In any event, you should check any critical point out with a lawyer, because the laws do vary from one jurisdiction to another. They also vary from one time to another, as courts issue decisions, and other courts reverse them.

Investigative Powers

Generally, a private investigator must conduct his investigations without what we call "police powers." A witness is under no obligation to furnish him information. The investigator cannot charge a witness with "obstructing justice" as a police officer can. He cannot obtain a warrant for arrest or search. Each state has its code of rules for private investigators, and they tend to be one-sided. A private investigator is not a cop, purely and simply. He must, moreover, report any information regarding criminal activity to the police, but they're under no obligation to inform him of any matter pertaining to a case upon which they're engaged.

Law of Arrests

A private agent can only make a "citizen's arrest." This comes from common law and allows any citizen who witnesses a crime to arrest the perpetrator. The police, on the other hand, can serve an arrest warrant. They can arrest on "probable cause," but this is somewhat vague. A private agent cannot do either, as a rule. If he doesn't see the crime, he can't make an arrest. Trying to do so exposes him to serious legal liability.

Search and Seizure

The Law of Search and Seizure is complicated, especially for police. There are new court rulings almost every day, modifying the rules dealing with the circumstances in which they can search a suspect and his property. For private investigators, it's much simpler. Everything's prohibited, except with the consent of the owner. In one sense, this isn't a serious limitation, because in industrial cases,

management gives consent to search, explicitly or implicitly. However, searching employees' lockers even on company premises is another problem, and may be forbidden in your state.

A curious exception to this is that, although your search is illegal, the evidence you turn up is admissible. Private agents are not limited by the same constitutional safeguards as are official police. You're liable for breaking and entering, but you can make a case with illegally-obtained evidence.[1]

Evidence

There are several different types of evidence, and various laws dealing with the obtaining and handling of evidence.

Direct Evidence is eyewitness testimony or any other that proves the claim directly.

Circumstantial Evidence proves the claim indirectly, such as a suspect's having no alibi during a questioned period.

Supporting Evidence doesn't deal directly with guilt or innocence, but supports the claim, as for example by demonstrating a motive, or an expressed desire to commit an illegal act.

Hearsay is not evidence. A third-party allegation that he heard the suspect admit guilt may be a useful investigative lead, but is not able to stand up in court.

A Confession can be introduced as evidence in many circumstances. This is the reason behind the Miranda Warning, in which an arrestee is advised of his "rights," the important one being that he does not have to give evidence against himself by answering police questions. The Miranda Warning does not apply to private agents, only to official

police. This is because the constitutional safeguards protect only against the government and its agents, not against a private citizen.[2]

Tainted Evidence is that illegally obtained. Although valid, it can be "suppressed," or thrown out of court, because it was obtained illegally. An example is a confession obtained through torture. Another is wiretap evidence obtained without a warrant. This applies mainly to the official police. As noted above, private cops have more latitude.

Physical Evidence is material such as fingerprints, tire tracks, etc. It's important to note that physical evidence can convict or clear a suspect.

You'll generally be seeking two types of information and material in your work: *investigative leads*, and *evidence*. Much information and evidence available to you simply won't be admissible in court. This doesn't mean you're necessarily unethical and taking short-cuts in obtaining evidence, but that by its very nature it isn't admissible, such as "hearsay." However, an investigative lead can allow you to develop evidence that will stand up in court.

An example is a rumor in the shop that a certain employee is taking company property. This isn't evidence, but can lead you to watch him carefully, and to arrange for surveillance when he leaves the workplace. This can turn up admissible evidence.

Another is a rumor regarding an employee who lives above his means. Living well is not a crime in any state, but lacking a logical explanation, such as inherited wealth or a rich wife, it can focus an investigation and lead to gathering evidence.

Bugging

Generally, bugging, wiretapping, and any other interception of communications are prohibited to

private investigators. The Federal Communications Act prohibits disclosure of the contents of any message, even if overheard accidentally and innocently, as in radio traffic. However, this law is almost impossible to enforce, for obvious reasons. State laws prohibit telephone wiretapping, except on a warrant, and judges don't issue warrants to private security officers. There is an exception — for telephone company investigators. They're allowed to tap phones merely on suspicion of a fraud against the telephone company. This is in the Omnibus Crime Control and Safe Streets Act of 1968. The telephone company, with its clout, managed to get this imprimatur from the government *without* attracting too much notice.

Federal law prohibits intercepting mail, except to postal inspectors with warrants. Laws against breaking and entering limit access to premises in placing a "bug," and some states have laws dealing directly with "bugs." These are easier to enforce because a "bug" is physical evidence.

Labor-Management Problems

Section 8A-1 of the National Labor Relations Act prohibits an employer from coercing or trying to unduly influence union activity. While the word "spying" is not in the language of the Act, court interpretations have held that this is inferred, and prohibited. An undercover agent who reports on union activity is violating the Act.

Sometimes, there's an arrangement whereby the employer hires an undercover agent to investigate what is nominally a criminal case, an accusation of theft, but is really a cover for a union investigation. This is very hard to prove, and the chances of getting away with it are good.

In real life, employers don't often have to engage outside undercover agents to penetrate a union. There are enough willing spies in the work force. These will take advantage of a union crisis to try to score points with the employer by reporting on fellow employees. These are amateurs, but there's really no need for a professional because the task is simple enough. Attending union meetings and striking up conversations with other employees to discover their sympathies isn't difficult. Because they've been working since before the start of the crisis, company spies have a very good view of the events, and already know the alignments of their fellow workers.

Entrapment

This is the big no-no. Inducing someone to commit a crime is illegal. It's important to note what constitutes "inducing," though. Providing the opportunity is not inducement, under the law. Leaving property unprotected does not allow anyone to steal it with impunity. Entrapment involves negotiations to persuade someone who otherwise would not have committed a crime to do so. To defend against a charge of entrapment, it helps if you can show that:

(1) The accused had prior convictions for this offense.

(2) He repeated the act several times.

(3) He committed the act in front of others, or dealt in an illegal transaction with others.

(4) You did not participate in the crime.

Experienced undercover operators know how to finesse their way around the prohibition regarding entrapment. There are ways of subtly suggesting that a crime might be worthwhile. The operator

merely has to pick out a likely target and say something like this: "Boy, anybody could make off with that if they wanted," and wait for the reaction. This is part of the "roping" technique.

Conclusion

There are legal "ins-and-outs" which you must know before starting an undercover program. On the one hand, you want to avoid becoming liable to prosecution. On the other, you may want to develop evidence that will enable you to prosecute someone else. In this regard, some of the points listed above show the contrast between employing a private citizen for your purposes, and hiring an off-duty police officer. The officer is limited by certain constitutional safeguards that don't restrict the private citizen. The officer has certain police powers which don't vanish when he goes off-duty. Balancing your needs against the situation will help you make the right decision. To be doubly sure, consult your lawyer, because the law may be different in your locale, and court decisions are constantly changing the interpretations.

Sources

1. *The Private Sector*, George O'Toole, New York, W. W. Norton Company, 1978, p. 12.

2. *Ibid.*, p. 12.

RECRUITING AGENTS

Recruiting an agent or informer can pose a problem. Much depends on the candidate's motive. In the case of an employer seeking a trusted employee to help him uncover theft, his candidate may be a very honest person with strong company loyalty, who resents anyone taking advantage of his boss. This is the ideological agent, and usually this sort is very reliable. In espionage, the same principle applies. A spy or traitor who works for the opposition out of ideology will be loyal unto death.

On the other hand, a recruit with an investigative agency may be a failed cop, a person who didn't make the grade for acceptance into the police department but who still wants to do investigative work. This brings up the danger of excessive zeal, in which the undercover person may fake evidence to "make the case."

Some recruit their people from military police or intelligence agencies. There are many short-term agents who leave the military after their enlistment periods end, and these are a pool of potential talent for private agencies. More important than their police or intelligence backgrounds is why they left. One obvious possibility is that they were unsuccessful in the field, and the prospective employer must be careful not to take such a background at face value. It may not be a qualification at all.

The most common motive with a private agency is, of course, money. The agents seek to earn a living, and are interested in making as much as they can. If the agency has an incentive system, very common in this private-enterprise-oriented country, it will pass out bonuses for productivity. Such bonuses can be irresistable temptations to a hungry agent.

Money motivation is a loser. Police officers don't like to pay informers, because they know that, under the system of paying for information piecemeal, the informers are tempted to manufacture "intelligence" to satisfy their masters. There's an incentive to produce more, in order to get more payments.

Working a "twist" on an informer is a more reliable method. The informer knows that he has to pass only enough information to "get off the hook," and is less tempted to over-produce. This method is still not 100% reliable, as a desperate informer may "finger" someone else to take the heat from himself.

Checking reliability is an uncertain process, but the control must try, to reduce the chances of his getting bad information. A common technique is to have the agent go through a polygraph examination.[1] The polygraph is unreliable, and has been oversold, but many place their misguided faith in it. The main value of the polygraph is to intimidate the person who believes that it will unerringly detect any lies.

Another method of checking the suitability of applicants is psychological tests. This is slowly gaining acceptance among police organizations in recruiting of patrolmen. However, only about 39% of police agencies rely on psychological assessments.[2]

There's good reason for distrust of psychological assessments. One immediate and obvious one is that any tests or interviews only show the candidate's performance at the moment, and may easily not truly

reflect his personality. Another is that many tests aren't adequately validated, with a consequent loss of reliability.

The new computerized versions of psychological tests are quicker and cheaper, but no better, than their manually administered predecessors. Some small "psychological assessment" services offer these to police agencies, claiming that they are almost infallible. This is mere huckstering. No test is infallible, computerized or not, and any such claim is an outright lie.[3]

Assessing a potential agent is difficult, but one good guide is background. If the candidate has had successful experience in the field, he's more likely to work out well. Past performance is the best guide to future performance, although it sometimes fails, because of "burnout" and other reasons.

Another, better, but more expensive method, is to send in two or more agents, and cross-check their information. It's essential that the agents have absolutely no knowledge of each other's existence, to avoid collusion.

This practice, however, has led to situations, undocumented but believable, in which agents informed on each other, each thinking the other was a target.

The dictum; "It's hard to find good hired help these days," applies especially to agents and informers.

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, p. 16. Barefoot points out that undercover operators do try to entrap innocent people in order to better their positions, and that polygraph tests serve to discover these.

2. *Applicant Investigation Techniques in Law Enforcement*, John P. Harlan, Ph.D., and Patrick A. Mueller, J.D., Springfield, IL, Charles C. Thomas, Publisher, 1985, pp. 6-7.

3. The author's experience in this regard is worth relating:

At a Fraternal Order of Police Convention, there was a "trade show" displaying police-related products and services. One of the services, run by an ex-cop turned polygraph examiner and a Ph.D. psychologist, was a computerized personnel psychological "screening" service. The two operators had their computers with them, and claimed they could screen out unreliable and undesirable applicants at low cost with their tests.

One test was a simple, pre-employment questionnaire. The other was a long clinical test that had been originally devised for use with mental patients. Both were true-false types. When I asked them what prevented an applicant from simply lying, they claimed that the tests had built-in "lie scores" to detect untruthfulness. These were based on the assumption that there are no perfect people: there's something wrong with everybody, and anyone who claimed not to drink, worry, become depressed, or have any other faults, was obviously being untruthful. One of them, the ex-cop, invited me to take one of the tests. I agreed, warning him that I intended to "dive-bomb" it. I sat down at the computer and punched in my answers to the questions, lying discreetly but significantly. The evaluation, which printed out a few minutes later, showed me quite truthful and employable, but with a problem driving record. Perplexed, the individual asked me to take the test over, this time being truthful. I did, and the printout showed me to be alcoholic, prone to drug use, uncooperative, and generally unemployable.

His partner, the psychologist, asked me to take the clinical personality test, answering truthfully. I did, and found that I'm sociopathic, perhaps even needing institutionalization.

As a check, I showed the printouts to my wife, asking: "Is this really me?" She scowled and handed them back, unimpressed. Showing them to two former employers for comments provoked laughter and ridicule of the testing procedures.

This is why it's necessary to be extremely cautious with psychological methods of assessment, computerized or not. They deal with intangibles, and can easily result in rejection of some very suitable candidates. In fact, they tend to be biased because they're derived from institutional backgrounds, and tend to be pejorative. In simple language, they show what's wrong with a person, not what's right, and they usually exaggerate.

TRAINING THE AGENT

Except for government operations, training of agents is done on the cheap. Private companies, ever paying attention to the budget, skimp on training. When we read of CIA training camps, with their month-long courses, the contrast with private efforts is striking. A security agency will spend perhaps four or five days in training an agent, at most.[1]

Training is unsystematized. It usually consists of having the trainee read reports of cases and then practice writing reports himself.[2] In reality, this doesn't teach him how to work a case; it teaches him how to write reports.

One very important reason for the scanty training is that many believe agents are born, not made. It's convenient to believe this when faced with the profit motive, and the need to earn as much as possible with minimal investment.

Another reason for the hurried training of undercover agents is that it must always be individual training. "Need-to-know" limits the class size to one, to prevent each agent from knowing the identities of any others. Individual instruction can be very expensive.

For anyone interested in providing good training for his agents, the job can be broken down into separate tasks, and the recruit can polish his skills in each one.

One skill which is both essential and easy to polish is interviewing technique. An agent who will work undercover at a workplace must apply for the job in the same way as other applicants. If the personnel manager or foreman isn't in on the secret, the agent can expect no help there, and must maintain his cover and appear good enough to be chosen for the job.

Training in interviewing skill comes in three phases. First, the instructor runs the recruit through a role-play, interviewing the recruit for a hypothetical job. He notes only any deficiencies, and after the role-play is over, advises the student how to correct his problems. He then sends him out to practice, applying at employment agencies and company personnel offices for real jobs. In so doing, the student agent can put down anything he wishes on the application form because the purpose is to practice interviewing, and putting himself across convincingly face to face. Applying for a position for which he's totally unqualified will test his ability to the utmost. If he can convince the interviewer that he really is what he says he is, that's good enough for the purpose of training. In time, a reference check would expose him, but as he'll fill in a false name and address on his application, this is of no importance.

This system costs the instructor nothing except the student's salary. The many unwitting personnel people whom the student contacts serve as sparring partners, at someone else's expense.

The third phase is to run through another role-play, when the instructor appraises how well his student has learned the technique.

Instruction in the technique of "roping" can be a short briefing, and a dry run. The instructor assigns the student to spend some time in bars, and to produce written reports on any information he's

been able to glean. Another method is for the student to pretend to be a salesman, visiting companies and attempt to extract information from the people he contacts. The reports should also contain the student's account of how he steered the conversations, and his reasons. This will give the instructor an idea of how well the student understands the basics. A final role-playing dry-run will help the instructor judge whether his pupil has developed enough skill in roping.

The ability to shake a tail can be important in the proposed assignment, if the agent will have to have personal meetings with his agency control. The instructor can give the student a basic lecture in the techniques of tailing, and start him off on the other side of the process, by having him tail people pointed out to him. The student's task will be to follow them home and report the name and address. This gives the instructor a dual opportunity: he can appraise his student's skill, and also his truthfulness and reliability. Telephoning the subject of the tail on a pretext can establish if the student is reporting correctly.[3]

The next step is to test the student's ability to shake a tail. An experienced and overt investigator will tail the student, without his knowing that he's the subject of the exercise. The only briefing the student will get is at the start of the tailing phase of instruction. This will determine the student's alertness, especially as the tail will follow the student while he's tailing someone else, or after normal working hours, when he's likely to relax his guard.

An orientation regarding the types of undercover assignments possible will give the student a good perspective, even if he never has to perform all of them. The instructor should lay them out for the student, briefly describing them and their relative degrees of risk and difficulty. The simplest type of

undercover work is area coverage. The agent establishes cover, living or running a business in the area, for general surveillance. One example was that of two British Army enlisted personnel, who set up a laundry in Belfast for intelligence purposes. The clothing they handled for their customers was examined for traces of explosives or cartridge propellant. This was valuable in furnishing leads for investigation.

It was also dangerous. Somehow, members of the IRA discovered their affiliation with the British Army and assassinated one member of the team.[4]

Another area in which undercover assignments come about are cases of insurance fraud. A claimant may have been disabled, and even have medical evidence regarding his disability. Planting an undercover agent in the area may disclose that the claimant is actually not as disabled as he says. The agent can secretly photograph or videotape him walking, running, or mowing the lawn to prove the case.

Employment is one of the most common types of undercover assignment. Because other chapters deal with this extensively, there's no need to go further into it here.

Infiltration means joining a group, and a deeper involvement than simple employment. Often, the target's a criminal gang, and the risk, if discovered, is high.

Spying, in the classic sense, is even more difficult and risky. Not only can there be a physical risk, but a legal one. In many instances, corporate espionage is vulnerable to at least civil prosecution.

Impersonation is extraordinarily difficult.[5] Few attempt it, and this sort of assignment is not likely to come an agent's way in a lifetime.

Individualized instruction has one great advantage. The instructor can tailor it to the needs of the student and the case. A part of the training will be an ad hoc briefing, in which the instructor will lay out the assignment to the agent. He'll provide a sketch of the personalities involved, the nature of the assignment, particular points to watch, and the nuts and bolts of how and how often to report, what information to seek, and other important details. The instructor can refer the student to written materials to save time. As noted above, having him read operational reports will show him the format desired, and having the student write a few himself, dealing with his practice assignments, will demonstrate whether or not he understands. There are various investigative manuals which can aid in providing a detailed briefing.[6]

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975 pp. 19-21.

2. *Ibid.*, pp. 20-21.

3. By pointing out people leaving a store to the student, the instructor can always later phone the subjects and claim that he's the store manager trying to return an item lost by that person. If the person denies having been in the store, this shows that something is seriously wrong. In this regard, it's important to note that people who are suitable for undercover work have to have a talent for deception, and that some of them may be practicing deception upon their employers. A symptom that appears early in the process suggests that the student, if allowed to continue, might be filing spurious reports when he goes operational.

4. *The Making of a Spy*, Raymond Palmer, Crescent Books, 1977, pp. 32-33.

5. *Methods of Disguise*, John Sample, Port Townsend, WA, Loompanics Unlimited, 1984, pp. 127-138. Trying to impersonate someone to his friends and associates is almost impossible. It can work if the target has never met the person being impersonated, but only knows him by reputation or by correspondence.

6. *The Investigator's Handbook*, Walter M. Strobl, Boston, MA, Butterworth Publishers, 1984. This book is full of checklists on points to watch in an investigation, as well as detailed information on types of characteristics of crimes that come under investigation. While the title suggests that it's of interest to an "investigator," much of the book contains information useful to the undercover agent and his tasks. There are detailed explanations of different types of businesses and their organization, methods of theft and fraud, and lists of loopholes in security upon which the undercover agent can report. A few chapters on traffic investigation, report writing, narcotics, and related subjects round it out.

BRIEFING FOR THE ASSIGNMENT

There are many nuts-and-bolts details that the undercover agent must have before starting. The supervisor or "control" must make sure to brief him thoroughly, as any omissions can result in serious repercussions.

The first item is the nature of the task. This isn't as simple as it might seem. One vital point, for example, in an employee theft investigation, is whether the client is seeking to prosecute, or merely to discover the thieves. This will determine the way in which the undercover investigator goes about his job. If the need is to prosecute, he'll have to be diligent in gathering evidence.

The client may not want to prosecute, for several reasons.[1] Bringing in the police means publicity, and sometimes company policy frowns on this. A prosecution can also impede other, contemporaneous, investigations. In a prosecution, the undercover agent is usually "blown," because he has to appear in court to give evidence. Finally, prosecution using an undercover agent opens up a possible defense of entrapment, which is a can of worms. Such a defense often depends on whose word the jury accepts, and if the defendent has a better courtroom presence than the undercover agent, there can be an acquittal.

For these reasons, management often feels that *firing for cause is the preferable course. In one sense,* punishment is swift and sure, and the deterrent effect on other employees is part of the rationale.

Sometimes, the assignment is not criminal, but in a category some call "employee misconduct."[2] Drinking on the job, using marijuana, sexual deviations, and simply goofing off are not necessarily criminal offenses, but may be against company rules. In such instances, internal disciplinary action, possibly including discharge for cause, is the only recourse open to the company.

In other instances, the investigation may concern employee efficiency. Retailers hire undercover shoppers to pose as customers and observe the sales clerks. They note if they're courteous, give prompt service, and handle requests for information or sales quickly and efficiently. They also note if any employee rings up false sales or short-changes customers. This shows that the dividing line between a criminal and a lesser investigation is very thin, and in fact they often overlap. In some jurisdictions, for example, smoking one marijuana "joint" is not a crime, but possession of a larger amount is.

There are administrative and tactical points to cover:

Expenses

Understanding the expenses allowed is important. How much "walking around money" does the agent get? Are there moving expenses? How does he replenish his expense money? How often does he make contact? With whom? By mail? Phone? Can he remember the number, or must he write it unobtrusively?

Contact

In a touchy assignment, making contact can require special security measures. Phoning from home is out. The line might be tapped. Phoning the security control at home is wise, and doing it from a public phone is best. In some cases, there will be a special number to phone, attended by an answering machine, to tape the agent's reports for later transcription.

There may be a need for an emergency contact procedure. The quickest and most convenient way is to use the telephone — an emergency number, manned 24 hours a day by someone who is familiar with the case and can get in touch with the control at any time. The emergency contact procedure may be a code phrase, such as "I heard your sister's sick," in case the agent may be overheard.

Reports

There will probably be a need for written reports. Where does the agent write them? To whom does he send them? How often? One source suggests issuing stamped envelopes to the agent.[3] If they're also addressed, they can be compromising, especially if the agent carries them with him for convenience. For security, it's best to issue envelopes and stamps separately, or have the agent buy them as he needs them. Americans normally don't write many letters, and a supply of ready-to-mail envelopes is sure to arouse curiosity, especially if they're addressed to "XYZ Investigative Services."

Using a "live drop" is a fairly safe way of sending written reports. The addressee should not be an employee of the agency, as a superficial check would disclose this fact. A mail forwarding service isn't

secure, because the discretion of the service owner is uncertain. A paid receiver, or a relative or friend of a member of the agency are the best possibilities.

Another point to watch is not to have a return address on the envelope.[4] This can blow the cover if for some reason the envelope comes back to the agent's address.

In some instances, personal meetings with his control may be part of the task. Going to such a meeting requires getting rid of possible "details." The agent should have gotten some training in tailing and counter-surveillance during training.

Company personnel are part of the picture, and the agent must know if he's authorized to contact anyone at the company, even in an emergency. This usually isn't the case, but the agent should know who knows about him at the assignment.

He must know where to apply for the job, and be rehearsed in the details of his cover identity, if any. If there are any special instructions about living accomodations, now is the time to give them.

Once hired, he must have a list of suspects, or at least an area to investigate. He must never know if there are other agents already placed with the assignment. This is particularly important if the undercover assignment is with a criminal gang. What he doesn't know, he can't divulge.

Sometimes the briefing takes many days. If the agent's required to relocate to an unfamiliar city, he needs time in which to find a place to live and to become familiar with the locale. Working an interim job can be useful, as it gives maximum contact with the residents, and gives the agent a "feel" for the locale.

One point which no source treats adequately is what to do with a failed assignment, such as when an agent fails to be hired. Does the investigator

abandon the task, or does he try to send in someone else? Before he can decide, he must find out the reason for the failure. Sometimes it's obvious, as when an agent inadvertently "blows" his cover. Sometimes, it's more subtle.

In some cases, applicants take an ability test.[5] Too high a score for the job can result in the applicant's being judged "over-qualified," and not getting hired.

Debriefing

Having the failed agent report back and going through a thorough debriefing can pave the way for a second try. However blatant the failure, there's always some information he can bring back with him that can be useful in a second try.

Sometimes the personnel manager, if he's not in on the secret, can be a serious obstacle. One way to handle this is to bypass him to bring in the agent, claiming that he was hired from a temporary agency. This isn't the best cover, but if it's all that's available, it may have to do.

Another way is to send the personnel manager on vacation, or on a special assignment, to get him out of the way. This can work with almost anyone who gets in the way, and is the prerogative of the company executive who engages the investigative agency.

The problem of pay needs handling in a way that won't compromise the security of the agent. Does he keep both his security agency and company paychecks? He can cash or deposit his company paycheck openly, but his other one can compromise him. Does he need it to live? Can the agency deposit it into his account by mail? Carrying a bank card, checkbook, credit card, deposit slip, or other financial document can blow his cover.

The briefing is necessary preparation for the assignment. Skimping on it can be as harmful as skimping on training, and compromise the agent.

Sources

1. *The Process of Investigation: Concepts and Strategies for the Security Professional*, Charles A. Sennewald, Boston, MA, Butterworth Publishers, 1981, p. 51.

2. *The Investigator's Handbook*, Walter M. Strobl, Boston, Butterworth Publishers, 1984, pp. 81-88.

3. *Ibid.*, p. 150.

4. *Fundamentals of Criminal Investigation*, Charles E. and Gregory L. O'Hara, Springfield, IL, Charles C. Thomas, Publisher, 1980, p. 225.

5. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, p. 38.

ESTABLISHING COVER

The need for cover depends a lot on the nature of the assignment and the people involved. If the assignment requires infiltrating a company to discover employee theft, the cover needed will be superficial. If the nature of the work is unskilled, or low-skilled there's no need to establish a deep background.

If the work is skilled craftmanship, cover will be more difficult. One authority writes of having the agent work for a few months in another job in the new city, and then apply at the target company.1 This is mostly nonsense. It's usually not possible to learn a skilled trade in a few months. In many skilled trades, it seems that everyone knows everyone else. Anyone with only a few months' experience will stand out. There are exceptions in cities with large transient populations. In such cases, it's normal for someone to "blow into town" and seek a job.

Experience in the trade is necessary, and faking it is difficult. Employees may have worked at the company the applicant claims on his record, or may know someone who still does. A casual word can blow the cover. Experienced employees can also easily tell if someone actually has the skill for the job.

In infiltrating the world of crime, it's almost as difficult, sometimes more dangerous, and establishing cover takes somewhat more work. It's necessary

to construct a criminal record for the agent, and to backstop it.

Backstopping

Superficial cover is sometimes as simple as assuming a new identity, without any corroborating documents. This will sometimes do, because the subject of the investigation isn't likely to ask to scrutinize the contents of the agent's wallet. In a drug assignment, for example, leaving the badge home usually suffices. In other instances, deeper cover is necessary. A few business cards, which most people accept at face value, is enough for an area assignment.

An agent who infiltrates a workplace will have to contend with a long-term assignment, during which his cover will have to stand up. The depth of the cover required will depend on the thoroughness of the investigation the opposition is likely to make. An agent who claims to have worked at another company should actually have worked there, or put on his application the name of a supervisor who will tell any callers that he did. If he claims to have lived in a certain city, he must actually have done so, although not necessarily for as long a time as he claims. He may well meet someone who asks him questions about the locale, and if he doesn't know the name of the main street, freeway, or even if the city has a subway, he'll blow his cover immediately.

Document and background checks are rare in most investigations, and the agent usually doesn't have to worry about a fellow employee visiting his alleged old neighborhood to verify that he actually attended school there. A falsified drivers license can be a problem, but not because of fellow employees. A cop who calls for a license check by radio will immediately spot a forged license, because the motor

vehicle bureau will have no record of it. This is why some backstopping is necessary, starting with a birth certificate. This enables getting other documents openly, and there will be the agency records to backstop them. One point to be noted is that obtaining any sort of official papers such as a drivers license under a false identity is illegal.

In criminal cases, it may be slightly more complicated than this. Sometimes, it can be as simple as inserting the agent's fingerprint card into police files, in the expectation that a criminal gang will have contacts in the police department to check the record. In the criminal world, background checking often entails finding mutual acquaintances who can vouch for the newcomer. Sometimes an informer can make the introduction and recommendation. In extreme cases, to build up the proper network of acquaintances, it will be necessary for the agent to serve time in prison to establish his bona fides. This will be on a fabricated charge, to which he'll plead guilty to shorten the process.

Once in prison, he can begin making acquaintances just by being there. Within the walls, he'll have a hard time being accepted at first, but with time, confidence will grow. Once he's released, he'll be able to use name-dropping, mentioning convicts whom he met in the "jug."

For most agents, the main part of their cover is simply hiding any connection with the police or company management. The truly hard parts are already done. They're American natives, speak English, and have lived here all their lives. The espionage technique of "pocket litter," carrying corroborating items such as bus and train tickets, isn't applicable here, as this doesn't involve infiltration of a foreign country or passing examination by expert counter-espionage police, such as the Gestapo. Although one source

recommends carrying corroborative papers, this is overkill. It's enough simply not to carry anything that conflicts with the role, such as a drivers license or credit card in another name.[2]

It's pointless, as we've seen, to try to place an agent who doesn't have the skill required for the job in a company. In criminal enterprises, the same rule applies, but it's not as obvious, because nobody has ever documented the job skills required for various criminal occupations.

In setting up a new identity for the undercover agent, it helps to have him use the same first name, to guard against the possibility that someone might call out his real name and he would respond to it. This could happen quite innocently, but anyone who claims to be "Jack —— " who turns his head when someone shouts, "Hey, Phil" would be suspected.

Attention to detail is vital. An undercover agent can assume that at some time or other he'll be scrutinized very carefully, and the basic framework of this new identity includes removing all traces of his former connections. Among other things, this means:

(1) Cleaning out his wallet, setting aside all credit cards, drivers licenses, Social Security cards, and any other identifying documents that don't fit in with his new identity.

(2) Not driving a car registered to his old identity or his company. Criminals do have contacts in official agencies, and having the plate number checked out is possible for a criminal with such connections. In states where vehicle registrations are public records, checking out a car is very easy. It can happen by accident, too. If, while driving with a fellow employee, the undercover agent gets stopped for a traffic violation, the police officer will routinely radio in a request for a check on the plate number. If

the name on the registration doesn't match the cover identity, this will blow the whole operation.

(3) The "need to know" principle is essential. Knowledge of the undercover operative's presence must go only to those people who need to know to help in the success of the operation. This means that, in the infiltration into a company, only one top executive in that company, the one who instigates the project, should know of it, and he should not share his knowledge with anyone unless there's no other choice.

(4) The agent should seek entry through normal channels. If the normal practice in hiring is for the applicants to go through the foreman, the agent can't have the personnel manager or president bring him down to the shop and announce that he's a new employee. This would be so out of place that it would be jarring, and would attract too much attention for the project ever to succeed.

This implies that the agent must be able to get the job on his own merits, not by "pull." Even if he were inserted into the workplace without arousing suspicion because of the method, he would not gain acceptance by the other employees if he were obviously unskilled and out of place.

(5) Part of the task of protecting a cover identity is to know as much as possible about the histories of the people in the group to be infiltrated. This helps to avoid conflicts. If, for example, the agent claims to be from a certain city, and to have attended a certain school, it would be compromising to have a member of the group confront him and announce that he lived in the same place, went to the same school, and didn't remember him. This applies also to the work history, as we have seen.

(6) Attention to detail is important in not blowing the cover. The agent's home must also be consistent

with his cover identity. He can expect to have some of his fellow-workers as guests, to cement the friendships, and if they see anything that contradicts the cover, it will be dangerous. Letters from the agent's relatives, if addresseed to his old name, can give him away. Luggage with the wrong initials is also compromising. A monogrammed handkerchief is a give-away.

The home must also fit the persona. A beer-drinking, blue-collar type will attract attention if his home has many works of art, or a piano. Bookcases can be give-aways, too, especially if the old high school album is among the books.

Maintaining the Cover

The undercover agent must be prepared to put in many hours on the job. His work doesn't stop when five o'clock comes. In most cases, the most important part begins. Socializing with other employees is vital, and the agent must be prepared to live his undercover life fully.

This demand on his time means that, if he's married, it will put a strain on the relationship. It also introduces the complication that his wife must also live an undercover life. If he has children, it can complicate the picture so much as to make it unworkable, as it's unreasonable to expect children to assume cover identities to match the needs of their father's work. The alternative is to live away from home for the duration of the task.

If he does this, the effect on his personal life can be severe. He has to leave his friends and relatives, and remain out of contact for the duration of the assignment. He can't receive mail, as the conflict in names would give him away. He can't save letters, or write to his relatives and friends, because if his home

is ever searched, the paper would give him away. This is one reason why bachelors and divorcees are preferable for the deep cover assignments.

The telephone is one way of keeping in contact, but this means he must place his calls from a public phone, to avoid tell-tale traces on his bill. It also minimizes the risk of a wiretap disclosing his identity.

Cover must be well-planned. It must be as deep and thorough as the assignment requires. Failure to watch the details can have serious consequences. This is the control's job, but also the agent's responsibility. He's the one who runs the risks.

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, pp. 36-45.

2. *D.E.A. Narcotics Investigator's Manual*, Paladin Press, Boulder, CO, p. 104.

INFILTRATION

Once there's a clear need for an undercover agent in a company, it becomes necessary to put one in place. There are several possibilities here, and it's necessary to examine each one to find the best solution.

Recruiting in Place

The first is to recruit someone who is already working for the company. This, a variation of the "informer" used by police, is the simplest way, because there's no problem in establishing cover or hiring an outside agency. The main drawback is that the employer may not be sure of this person's reliability or honesty. There have been cases of long-term employees, faithfully serving the company for years, "turning" and becoming dishonest. Another drawback is that the prospective recruit may not feel comfortable in "ratting" on his fellow workers. Yet another problem may come about if employee-management relations are strained. The employee might view any effort by management to recruit him as dirty pool, no matter how legitimate it may be. If there's a union, there's the danger of this effort appearing as a union-busting activity.

Finally, a suitable candidate among the employees might not be as suitable as he seems, because if the

employer trusts him implicitly, this may be apparent to others. He might have a reputation as a "company man," and therefore be unable to penetrate a group engaged in dishonest activity because the members will hold him at arm's length.

Hiring an Investigative Agency

Many private investigative agencies advertise openly that they do undercover work for companies. These agencies vary in levels of competence, and there's good reason to be cautious in choosing one.

Many of the agents are poorly-trained.[1] They get a week, at most, the sort of patch-up job that barely prepares them for this demanding task. Some of the larger agencies have traveling undercover agents, skilled specialists who go from job to job as needed. These are more expensive. They may also not be available when you need them.

If the agency is competent, the director of investigations will require a list of all your employees, and probably copies of their entire personnel files. This is to check out their work backgrounds, to ensure that there's nobody there who knows the undercover agent by another name, or worked at the same company during an investigation. Such a person could compromise the operation at the start. If one of your employees does know the undercover agent, the director of investigations might choose another agent, or he might ask that you fire that employee, leaving the pretext and the dirty work up to you.

The prospective agent would need the skill for the job, as inserting him otherwise would seem suspicious. There must be an opening. It's possible to create an opening by promoting or reassigning the person already working in the slot.

Hiring should go through normal channels, to avoid suspicion. In small companies, the owner often does the hiring himself, and this isn't a problem except that he must follow his usual procedure every step. If prospective employees normally fill out applications, the agent must also do this. Although much hiring is through the "hidden job market," by word-of-mouth, it will enhance credibility to advertise the job in the classified ads, and interview applicants.

If the company is large enough so that hiring is delegated to a foreman, or a personnel manager, it's necessary to take him into your confidence. "Need-to-know" is very important here, as is honesty. This means that you must be sure he's both discreet and not part of the subject of investigation. He places the ads, goes through the motions of interviewing the applicants, and makes the selection. There must be no obvious favoritism, and the applicant must truly be qualified for the job to avoid arousing suspicion.

For higher-level jobs in a large company, the Chief Executive Officer will usually do the hiring himself. This gives him the latitude to choose whom he wishes, and placing an agent is simpler. Finding an agent who can "fit in" and carry out the responsibilities of the job will be harder, though. Agents who can blend into a blue-collar workplace often won't fit into high-level corporate management. In this regard, the CEO can give direct help, especially if the agent reports directly to him as regards the formal table of organization. The CEO usually has the latitude to hire a "personal assistant," and define his duties which lets him adjust the job to the agent's skills and to "cover" for his shortcomings. This can only go so far, though, because to be sucessful in the undercover role, the agent has to be able not only to do the job, but to be accepted by others. If he doesn't seem to "fit in," to

share their values, backgrounds, and attitudes, he won't become part of the group.

Once hired, the agent must appear to be just another employee. He will make his contacts through his agency, not through you, and you'll get your reports from the agency.[2] The quality of these reports will depend very heavily on the intelligence, skill, and diligence of the agent.

Do-It-Yourself

You might decide the best course is to work your agents yourself, from recruiting and hiring, through the many weeks or years of case-work. Some of this will fall into your lap. In most groups of employees, there are some who are willing to do "favors" for the boss, to further their ambitions. Exploiting these, while cautioning them to be discreet, will accomplish the purpose. If you're lucky enough to find an employee who is willing to do this because he's basically ethical, or out of loyalty to you or the company, count your blessings and make the most of him.

This is a long-term plan. In this regard, it's better to have an agent in place before the need comes up than to try to insert one, from whatever sources, after the problem arises. There is a danger, of course. You'll have to draw from the same human material as for your other employees, and you may get an unpleasant surprise. Your trusted agent may turn dishonest after many years. This is why he must never go solo. Having two or more agents, each believing he's the only one, is a good way to ensure reliability. Cross-checking their reports will give you a good idea of their quality and honesty.

Discretion is important, not only to conceal the true activity from possibly dishonest employees, but from other agents. Your agents must never get

reputations as "company men." They should not show an overly-friendly attitude towards you, and you should not be overly-familiar with them "on company time." They must understand the need for this, and know you can make it up to them in other ways. Secret meetings or phone calls are common ways to maintain contact.

Whichever way you choose to get your undercover agents, infiltration will be a barrier you must overcome to ensure success. It's a continuing task, because infiltration doesn't stop once the agent is hired. He must maintain his cover and work his case without compromising himself.

Infiltration in Other Contexts

A classic private undercover infiltration began in 1873, when there were labor-management problems in the Pennsylvania coal mines.[3] The Pinkerton Detective Agency, which had a number of railroad companies as accounts, took on the task of fighting the "Molly Maguires," which would have been called a "terrorist group" had the term been in vogue at the time. An undercover agent, James McParland, gravitated to the area and found a job under the name of James McKenna. He gained the confidence of the other workers, and was able to infiltrate the Molly Maguires. He worked undercover for three years, gathering information for investigative leads and evidence for prosecution. His assignment was dangerous, in the sense that if his true role had come to the surface, the Molly Maguires would have had no hesitation in disposing of him. However, they were relatively unsophisticated, and McParland/McKenna was able to continue his undercover work unsuspected.

The underground press had a series of articles on "Tommy the Traveler" in the late 1960s. "Tommy"

was apparently a government agent, a mobile infiltrator who went around the country posing as a "peace activist" and infiltrating various local movements. He became well-known, with his photograph published in various sources, but his true identity never came to light.

The various enforcement arms of the U.S. Goverment have many such traveling undercover agents. They infiltrate criminal gangs and organized crime. Some concentrate on terrorists. Understandably, they receive little publicity, and because of their mobility, they don't become too well known. Whenever the cover wears thin, the parent agency pulls them out and re-assigns them.

One fascinating autobiographical account tells of a U.S. Secret Service agent who spent much of his time undercover.[4] A good deal of his work concerned counterfeiters. A reading of his book gives many interesting details of the undercover life. We find the need to keep a low profile, and still know when to be assertive. Motto had to learn the criminal argot to fit in. Reading between the lines, we see how he took some short-cuts with procedure, bending the law slightly to make the case. Although Motto didn't write it as a textbook, it's a very worthwhile guide to the realities of undercover work during that era, and many of the principles Motto applied are valid today.

Police investigation of various sorts of white-collar crime involves some undercover work.[5] Direct penetration is not as valuable or effective as other techniques. Some of these operations involve selling fraudulent "deals." This offers an opportunity for an operative to seek work as a salesman, learning first-hand the deceptive practices for later evidence. He can testify that the people running the operation instructed him to use deception in "selling" to customers.

Another way is to infiltrate as a victim. Many real-life victims are unwilling to come forth, because of their shame at having been outwitted. An undercover operator, using very thin cover ("leave the badge at home") can pose as a client, responding to advertisements and attending the sales presentations. The only special technique needed might be a concealed tape recorder, to confirm his testimony if the sales pitch is crooked.

Another technique is to join fraudulent religious organizations, send away for quack cures or present oneself directly for "treatment."

A news organization infiltrated Chicago's nether world to gather information for what became both a newspaper expose and a segment on the TV show *"60 Minutes."* During the time they operated a real bar for other purposes, they encountered corrupt city officials, an accountant who instructed them on how to fudge their books to show lower earnings, a "business broker" who knew all the angles and earned the title of "Mr. Fixit," and a crooked fireman, among others.[6]

We see that infiltration takes many forms. The agent can be employee, victim, customer, bystander, and play many different roles. The cover can be superficial or deep, and the infiltration can serve many purposes, from information-gathering for a news agency to various sorts of criminal and civil prosecutions.

Sources

1. *Undercover Investigation*, J. Kirk Barefoot, Springfield, IL, Charles C. Thomas, Publisher, 1975, pp. 19-21.

2. *The Investigator's Handbook*, Walter M. Strobl, Boston, MA, Butterworth Publishers, 1984, pp. 6-8.

3. *Surveillance and Undercover Investigation*, Art Buckwalter, Boston, Butterworth Publishers, 1983, pp. 128-129.

4. *Undercover*, Carmine J. Motto, Springfield, IL, Charles C. Thomas, Publisher, 1971.

5. *The Investigation of White-Collar Crime*, Law Enforcement Assistance Adminstration, U.S. Department of Justice, April, 1977.

6. *The Mirage*, Zay N. Smith and Pamela Zekman, New York, Random House, 1979.

ROPING OR GAINING CONFIDENCE

In any group, it takes time for a newcomer to gain acceptance. If there's a criminal enterprise involved, there's deep suspicion of any "outsider" and a standoffish attitude on the part of the established members of the group. Only when the newcomer is no longer a newcomer will he have a chance to get into the inner circle.

Often, the first sign of acceptance will be an invitation to have a drink with the boys after work. This can lead to a closer acquaintance, if the agent plays it right and doesn't try to rush it.

There are two techniques to speed up the process of acceptance, and neither one is under the control of the agent:

(1) *Have more newcomers arrive.* A company may be hiring many people, and this makes the agent an "old hand" or "regular" more quickly than if he had to compare his seniority with those who have been there twenty years. Some companies have high turnover rates, which helps this process. Other companies have very low turnover, and it will take much longer for a newcomer to gain acceptance.

(2) *Send in a decoy,* an agent who makes himself conspicuous by asking indiscreet questions, by listening in on conversations, looking in drawers and toolboxes, and trying to get too friendly too soon. This will draw attention away from the real agent.

When the real agent has gotten an "in," the decoy can leave, his job done. Nobody will miss him, because it was his task to not "fit in."

The problem with this method is that in some instances the decoy, especially if he does his job too well, may suffer for it. In a blue-collar environment, antagonisms are often settled on the loading dock or in the alley. In a white-collar milieu, there's less chance of violence, but there can easily be more suspicion.

Gaining confidence, or "roping," is a subtle process. It involves letting the targets know your values and attitudes are similar to theirs. The behavior required is the same as that needed to be accepted into any group, illicit or not.

First, it's necessary to keep a "low profile," not attract undue attention to yourself. Normally, a newcomer attracts enough attention.

Adopting a friendly, approachable manner to all you meet helps your eventual acceptance. In undercover work, there's no room for personality clashes, because these can stand in the way of gaining valuable information or contacts.

Part of the technique of demonstrating shared attitudes is to try to share after-hours recreation. If the norm is to "stop off" for a drink, join in, but don't get too affected by the alcohol. A bowling league might form the core group of a theft ring. The possibilities are endless. Realistically, this is one of the limitations. An undercover agent can't be everywhere, know everybody, and do everything. Using good judgement will help pick out the most productive activities, but one agent may not be able to cover all the possiblities.

In a criminal gang there are some additional techniques to speed up acceptance. One is to have a "turned" member vouch for the undercover agent.

This has its benefits, but also its great risk. The turned member must be fairly reliable, because he literally holds the agent's life in his hands. If he turned once, he may turn again.

One way of minimizing this risk is to have him arrested shortly after he helps establish the agent with the gang. This is hard to do while keeping him utterly incommunicado, and there's still a risk that he might change his mind and pass the word. His arrest also might lead to an interpretation that the agent had something to do with it.

Fortunately, there's a safer way. It's now common practice to relocate and disguise witnesses and informers. The Federal Government has had such a program running for over two decades, and some local agencies have followed suit. This enables the person to drop out of sight, and as this is a voluntary process, it's relatively easy to keep the person incommunicado. The handlers can bolster his fear, persuading him to keep his head down, by feeding him false "intelligence" reports that there's a contract out on him.

Dropping out of sight doesn't necessarily mean the other members will see him as a snitch under police protection. He can, before he disappears, let out a cover story that he's relocating to another part of the country for family or other reasons, thereby avoiding stigmatizing the agent.

There's yet another way to get rid of the embarrassing presence of the helpful snitch. In large cities, unidentified people are involved in accidents fairly often. The police can make it appear the snitch died in an accident. Arranging this can be difficult, because the accident must have been such that the body is not recognizable.

Normally, it won't be possible to use these techniques, and the agent must proceed slowly, but

surely. The basic principle is to keep a low profile, to blend in with the crowd, and not be too aggressive. The required behavior is exactly the opposite of that shown by the decoy agent, mentioned above.

There should be no overly intense rush to establish friendship. This can lead to rejection. It's best to keep fairly quiet, and simply do the job, without becoming personal with anyone at first.

In a workplace, there's always curiosity about a newcomer. Sooner or later someone will sidle up to him and ask some casual questions about his work experience and his personal life. This person is usually the company gossip, and such attention doesn't necessarily signify suspicion. He may be invited for a drink after work. This offers the opportunity to do some roping.

Roping involves getting established with the group and eliciting information subtly. The skilled roper will not ask direct questions, knowing this would be indiscreet and excite suspicion. Instead, he'll wait for the subject to come up. In some instances, he can speed up the pace by revealing damaging "information" about himself during the drinking session.

One way of doing this, if investigating a theft ring, is to tell his target that he was once fired from a job for stealing. He can go on by saying that he felt he was justified in stealing from his company because the wages were so low that he felt that he "had it coming to him." This fits in perfectly with the "unwritten law," and may provoke a response from the target. At least, it will show a degree of trust the agent places in his target by revealing this damaging information, which presumably is not on his employment application.

This also shows a similarity in values between the agent and his target. Most people who steal from

their employers don't see themselves as bad people. They feel they're just "getting what's mine," and taking unofficial compensation from the company.

The technique of roping is exclusively interpersonal relations. This is a skill that most people develop naturally, and some become very good at it. The prevailing view used to be that this skill is inborn, and one agent of the old school became very good at it, and concluded many successful cases.[1]

The new view is that this skill can be learned.[2] This is reasonable, because the "art" of roping is really an interplay of verbal tactics. To understand it, it's important to be able to think on your feet, and the new agent can develop this skill by role-playing. Repeated rehearsals can improve interpersonal skills, even the specialized ones needed for roping, and an enlightened training director will have such a program.

Sources

1. *Undercover*, Carmine J. Motto, Springfield, IL, Charles C. Thomas, Publisher, 1971. Motto had a long career with the U.S. Secret Service, running down counterfeiters, and much of it he spent undercover. He played his role so thoroughly that he was even arrested to keep his cover intact.

2. *Undercover Operations and Persuasion*, Randolph D. Hicks II, Springfield, IL, Charles C. Thomas, Publisher, 1973. The author shows how to learn this valuable interpersonal skill. There are dialogs demonstrating the right and wrong way to act in various scenarios.

EMPLOYEE THEFT

This is probably the biggest dollar-volume category of crime in this country. It easily outranks shoplifting because employees operate on the "inside," and know the employer's inventory, facility, and security system intimately. Contributing to this picture are some short-sighted policies by employers.

The Unwritten Law

There's an unwritten law that governs employee theft, one which both casual thieves and professionals follow. It's not found in religion, not descended from common law, not codified in any statute book, or case law, and many people ignore it. It's rarely admitted, and never documented, but it's no less real.

The unwritten law is very powerful, because this is what people actually do, not what they preach. The unwritten law varies somewhat from person to person, but it's approximately as follows:

(1) It's all right to steal from the boss, but not from a fellow worker. The boss is rich — he can afford it, but a fellow worker's knocking his brains out to make a living, just like you, and stealing from him is dirty.

(2) It's all right to steal from the company, because you're only getting back what they owe you, anyway.

They try to pay you as little as they can, and will dump you out the door in a layoff, so anything goes. It's a rough world, and you've got to look out for yourself.

(3) Everybody does it, in different ways. The foreman takes home pads and pencils for his kids to use. Another guy takes a can of oil for his lawnmower. The boss steals money out of the petty cash. He takes his friends to lunch and puts it down as a business expense. The higher-ups always do it. The purchasing agent's on the take from suppliers. The plant manager bribes the government inspector. Even the biggest names in government are dishonest, so who are they to tell me I've got to walk the straight-and-narrow?

(4) It's illegal, but only if you get caught. A lot of guys do it and don't get caught, and the bigger they are, the more they get away with it. The law hits the little guy. The big guy gets a smart lawyer, and is home free.

Part of the problem is that employers and legislators ignore this ethic. Perhaps they feel that recognizing the unwritten law will legitimatize it, and ignoring it will make it go away. This is obviously untrue. It never goes away, and the most striking aspect is that the employee who steals sometimes has a "Robin Hood" aura, and earns the respect of his fellows. Severe cynicism and demoralization among employees is very common.

Some companies, with enlightened policies and good relations with employees, have less trouble with theft than do others. Most companies don't have very enlightened policies. It's hard to demand loyalty from employees when company policy is against it. Expecting two weeks' notice from an employee who quits seems unreasonable when the company lays them off with one day's notice or less. Morale and loyalty are problems in most businesses.

No matter how good employee relations are, there will be an irreducible hard core of professional thieves who will steal simply for profit. These are a risk in any business. Some are thieves by opportunity, taking only when they can. A tiny proportion of them will take a job with the intent to steal right from the start, and they'll create opportunites.

Company security has several facets, and many employers ignore them, or make only token efforts. Briefly, they are:

(1) Check out prospective employees. Have they histories of job-related theft? Checking references carefully will help a lot.

(2) Limit the opportunities for theft. Tight security, without being oppressive, helps. A company that deals in small, light objects will provide temptations and opportunities.

(3) Have a decent security force. This is where most companies fall down severely. The security force has a heavy responsibility, and in principle they're the employees who carry the most trust.[1] Yet, they're often poorly paid and poorly-qualified.[2] Along with skimping on pay, the employer skimps on training. According to the Rand Corporation study, guards are typically ill-trained, most having no training at all. Most of the rest had eight hours' training or less. This applies even to those issued weapons. The contradiction is obvious.

Often, the guard force participates actively in theft. One night watchman, working on the New York waterfront, gave this account:

"Sure, we take stuff. When there's a shipment, the guys make sure they drop a crate or two. The crate busts open, and we get in and take stuff, and a lot of times, nobody ever knows. Say it's booze, we see broken bottles, and we take the ones that didn't

break. The insurance pays for it. The bosses don't care. Even guns. Once, a crate from Beretta came in. It got dropped. The guns slip in a pocket real easy. A lot were missing. The bosses knew they got kiped, but who could prove anything?"[3]

One authority recognizes this danger[4] and advises the undercover agent to note whether the guards talk with other employees, and are familiar with them. It would be surprising if they didn't. Guards are on the lowest rung, or near it, and there's no reason for them to consider themselves a privileged class, above the other employees. This is why undercover reports of guards talking with other employees are meaningless.

Employee theft isn't always nickel-and-dime. Sometimes, large amounts are involved. The 1974 theft of $3.9 million from Purolator is an example of an "inside job."[5]

Employee theft isn't limited to the blue-collar work force. The executives often steal more, not necessarily because they're less honest, but because they have access to larger amounts.

Companies who take it seriously will hire undercover agents, through an agency or their own security office. The far-seeing ones will have permanent or semi-permanent undercover operators.

Sources

1. *The Private Sector*, George O'Toole, New York, W.W. Norton Company, 1978, p. 44.

2. *Private Police in the United States*, James S. Kakalik and Sorel Wildhorn, Rand Corporation, 1972. Available from U.S. Government Printing Office.

3. Personal account by an acquaintance of the author.

4. *The Investigator's Handbook*, Walter M. Strobl, Boston, Butterworth Publishers, 1984, pp. 45-46.

5. *The Private Sector*, p. 15.

WORKING NARCOTICS

This chapter is here to give an overview of the task, but not in the expectation that the reader will actually need it. Some of the techniques tie in with those in other areas, and the reader can draw a few lessons from them.

The first point is to clear up misapprehensions. TV watchers may get the impression that narco cases are solved in an hour or less, after a burst of strenuous and dangerous activity. Actually, such cases are often frustrating, because they yield insignificant results, or wind up in dead ends.

Low-level penetration is easy. Dressed for the locale, an undercover agent can make a "buy" and this leads to the arrest of the small dealer. Progressing to a higher level is very difficult.

For this low-level activity, the agent needs to be "street-smart" and fit into the milieu. This means appropriate dress and language. It isn't necessary for him to have "needle tracks," because most illicit drugs aren't used by injection. The undercover operator may be a police officer, or a "turned" user. A common method of operation is for the agent to make a "buy," while a stake-out team stations itself nearby. Upon completion of the buy, the team makes the arrest. This is the "buy/bust"$_1$ and requires the least in time and resources. The agent needs some "front money," often less than $100 in marked bills, and the deal can be over in a few minutes.

It's simplest to use a "turned" addict. He knows the locale, knows the dealer, and often can make the approach without arousing suspicion. In this sort of situation, the police can use a "twist" to enforce compliance. He operates under their direct supervision, which simplifies the task.

An undercover cop has a somewhat harder time of it. Drug dealers are paranoid. Approaching them can be difficult because they don't accept strange faces easily. It's absurd to try to walk up and make a buy. It's necessary for the agent to hang around the neighborhood, and become known. Sometimes, it's possible to shorten this process by having a "turned" addict make the introduction, but this risks "burning" the addict.

Some dealers are so paranoid that they insist upon extreme measures to assure their safety. Some will ask the buyer to use the drug in his presence. There are several ways of getting around this. One is to claim the buy is for someone else. Another is to say the agent just took a dose before arriving, and won't need another for awhile. In the case of an injectable, the agent can say that he didn't bring his "works" with him, and doesn't want to risk infection from another set.

This paranoia can be such that the dealer will keep his stock stashed in hiding places away from his premises. He'll want to direct the buyer to another location to pick it up, once he has the money. The buyer can refuse, and insist on a direct cash for drugs transaction, feigning distrust.

Any undercover agent's career will be short-lived operating this way. In a buy/bust, the dealer sees the agent, and remembers. When he makes bail, he'll be out on the street spreading the word.

This is why the "walk-away" is also in use. This is delayed gratification, in which the agent makes the buy, and walks away. He may make several buys, and

the arrest follows later. Sometimes this is necessary for the prosecution to establish that the dealer is regularly in the business, and not making a one-time sale. The drawbacks to this are that it costs more money, and the police lose sight of the dealer. He may get spooked and flee, and the effort and money invested are total losses.

Front money is often a big problem. The smaller agencies simply can't raise the money to finance a big buy, which limits them to small cases. A large amount of money inevitably brings with it two problems: getting it, and safeguarding it.

In some instances, the small agency can have an arrangement with a local bank to furnish a short-term, interest-free loan, for use as front money. In other instances, a large agency may still not be able to obtain enough. Both have a choice, that of calling in a higher agency, such as the state police or the DEA.

This has its problems. Inter-agency rivalry, politicking, and empire-building all degrade the effectiveness of American police. When a smaller agency asks a larger one for aid, it faces the prospect that the larger agency will take over the case. At the very least, the smaller agency will have to work the case according to the larger one's guidelines, which may conflict with the smaller agency's policies or practices. In some instances, the larger agency will act very independently and ruthlessly. After the small one's staff have done all the preliminary groundwork, the larger agency will step in and take full credit for the success. From their viewpoint, this is necessary to justify their large appropriation, but people in the small agency will understandably be peeved. Next time, they may let a case go rather than hand it over. Inter-agency cooperation suffers.

Safeguarding the money is always a problem. The supposed buy may actually turn out to be a burn,

and the "dealer" may hold up the agent for the money. Another possibility is if the dealer tells someone else of the impending buy, and word leaks to a stick-up team. This is what makes the presence nearby of the stakeout team so important, and requires other security measures, such as choosing a location where it's possible to block escape and where innocent people are not likely to be present in case of a shootout.[2]

Another danger is that drug dealers are usually very unsavory types, who lie, cheat, and are more unreliable than most people. This is also true of narc informers, and often the police may have high hopes of making a case based upon what they're told, only to have it evaporate into thin air when the moment of decision arrives.

Getting to the higher-ups is often a laborious process. Cases such as the *French Connection*, with a chance encounter leading to a major interdiction and arrest, happen very rarely. Most often, it requires long and painstaking work. There's a hierarchy in the drug trade, and it's usually necessary to go step-by-step up the ladder.

An addict arrested during a burglary can lead to taking down a low-level dealer. The dealer, if the police can "turn" him, can lead to a wholesaler. The wholesaler has stronger security measures, because he deals with a very limited clientele that's well-known to him. He may simply refuse to meet with a stranger. If he does, it must be upon personal introduction. Even then, he'll often delay while he checks out the newcomer. This is why an observed buy is more productive than an attempt to infiltrate an undercover agent into the system. The police persuade the dealer to make a buy when and where they say, stake the premises out, and then make the arrest. This burns the dealer, but the price is worth it. The wholesaler will, of course, seek revenge, and

will kill the renegade dealer himself or by proxy, but to the police, the dealer's life isn't worth much, compared to the need to put the wholesaler out of business, and they willingly accept this risk.

Getting to an importer is almost impossible, for similar reasons. Such cases do happen, and they're invariably headline news when they do, because of their rarity.

The foregoing gives a picture of why, despite recent publicity, the police effort against drug dealers has been failing, and will continue to fail. In one sense, it's like the ill-fated prohibition on alcohol that brought about sensational newspaper headlines during the 1920s and early 30's. The use is too widespread, and "busting" a few low-level dealers hardly impedes the market. Undercover work is long-term and frustrating, and usually unproductive, despite the "narc" plainclothes officers who strut about with their airs of authority.

Sources

1. *DEA Narcotics Investigator's Manual*, Paladin Press, Boulder, CO, p. 101.

2. *Ibid.*, p. 103.

PROTECTING THE INFORMER

The normal practice among police units using informers is never to write down the identities of informers. It's very compartmentalized, and each detective has his corps of "snitches" which he keeps secret from his fellows. The reason is clear: "need to know." There have been some bad cops, working for the "mob," and letting out such sensitive information to fellow officers without an overwhelming need is dangerous.

Judges who sign search warrants recognize this, and often will accept an affidavit that doesn't mention the source of the information. Typically, the affidavit must state that the information comes from an informer, and that his informer has proven reliable in the past, which gives reason to believe that his information is correct for the case at hand. The officer producing the affidavit must affirm it under oath, but the conditions are such that the court has only his word for it that an informer even exists.

This can lead to abuses, the extent of which we cannot measure. It's a normal human trait to exaggerate slightly, to shade the truth to get desired results, and the amount of padding, or falsification, is up to the individual officer and his conscience.

We cannot measure the accuracy of affidavits. We can only assess the results, whether a search

discloses the needed evidence. It often does, leaving open the question of the way the information became known.

As a matter of general practice, the granting of search warrants based on affidavits depends more on the record and reputation of the police officer who swears one out than on his informers. One who has a good track record will find it easier to persuade a judge to sign one, while one whose record is poor will find it difficult.

Protection of the informer is paramount, but this protection can go into some dangerous areas. Usually, the informer is required to participate in crimes. If the informer is an undercover police agent, law or departmental policy may forbid him to take an active role in a crime. This is a weak point in the agent's cover.

A gang will usually have the newcomer go through a test before accepting him. This is to judge if he has the ability and fortitude for membership, and to screen out police agents. The result is that, if the newcomer is to gain acceptance, he must commit a crime and the police must condone it. The practice varies with the department, and the special unit involved, and there's no reliable information regarding how far police across the country are prepared to go.

There may be a blanket prohibition, as in the case of "Operation Red-Hot Poker," but this lends itself to circumvention, as we've seen. There may be a tacit policy of giving the investigative unit a free hand, with the police chief not wanting to know the exact methods his people use to get their results. This is what often happens in international espionage, with the political masters giving the secret service a "license to kill," as long as they don't know about it and the secret agents don't get caught. If they do, the

leader simply disavows them. The principle seems to be: "If you do well, you'll get no thanks; if you get caught, you'll get no help."

In some instances, the informer will have a license to commit crimes granted by the investigative unit, if this is the only way of keeping him in good graces with the group he's penetrating. In other instances, usually cases requiring long-range investigations, he'll be "arrested" along with the others, in order to establish his bona fides for a mission down the road.

An obvious fact is that the informer has to earn a living, and usually his livelihood is illegal. If the police unit has enough money to pay him a wage, the investigator can forbid his committing crimes. If the department's budget doesn't allow subsidizing an informer, the police can "look the other way," while the informer earns his living through crime.

Another aspect of granting immunity from prosecution occurs in "turning" a criminal, as we've already seen. There's an advantage in letting a small offender go in order to catch the "big fish." The police "cut a deal" with the offender, very unofficially, to extort his cooperation.

"Burning" an informer does happen, but it's hard to determine how often. A lot depends on the investigator, his skill, his relationship with the informer, and his eagerness to "make" a case.

Sometimes, it happens through carelessness, and this is not always casual divulging of the name. If the informer passes information to the investigator that enables him to make an arrest, the investigator may face the dilemma of proceeding with the case or letting it lie in order not to "burn" his informer. A raid will always produce the question, "Who talked?" among the arrestees. If the raid follows immediately upon the informer's learning the damaging information, he may be "burned." The "word" will go out on him, and he may even fear for his life.

Some investigators treat their informers quite ruthlessly, with contempt, and consider them expendable. They feel that an informer, a criminal himself, is among the scum of the earth, and deserves no consideration whatever. The limit on this attitude is that an investigator who "burns" his sources will soon find he has no sources left.

The investigator may not mind. Police officers know that "making" a big case is often the stepping-stone to a promotion, especially in police departments on the east coast, and may be quite willing to sacrifice an informer for that promotion. Generally, the promotion places him in a supervisory position, where he no longer needs informers of his own. This makes his snitches expendable.

All told, the life of an informer is dangerous. He faces a threat from the police on one side, and from the people on whom he informs on the other. He soon finds that he's gotten in more deeply than he realized, because his police officer control now has more leverage to "twist" him. The ruthless officer can ensure continued compliance by threatening to "leak" the informer's identity if he fails to cooperate. Some break under this relentless pressure. Many are unstable personalities at the outset. For these reasons, informers tend to have short and unhappy lives.

UNDERCOVER WEAPONS

Unlike the fictional, romanticized undercover agent, the real-life one rarely needs weapons. The stark fact is that if he must defend himself against deadly force, he's failed seriously and conspicuously at his job.

Very few undercover tasks involve any personal danger. Narcotics investigation is one, because clandestine narcotics dealers are both paranoid and violent. In most other areas, such as employee theft and labor-management problems, there is little prospect of violence. Embezzlers and counterfeiters aren't usually violent. Consumer fraud is non-violent. Most of these people aren't serious risk-takers, or they'd be trying their hands at bank robbery or kidnapping.

Why, then, the emphasis upon weapons? First, many of those who "carry" are police officers. Departmental regulations require them to be armed. There are exceptions for certain undercover tasks in which a weapon might be compromising.

Another reason is the "macho" image. There's a thrill in carrying a weapon, a hint of possible danger, and some people like this because it makes a dull job more exciting. Both police and quasi-police get carried away in this regard.

One detective sergeant I know carries a Bauer .25 ACP pistol in a wallet holster, although his job is

relatively safe. He runs undercover agents, one of his biggest operations being against a number of prostitution services, cited elsewhere in this volume. One occasion during which he went into the field, working "undercover" himself, he met with two truckers who had answered a classified ad he'd placed in the local paper. The ad simply called for a trucker to haul a load. When he met with the applicants, in a local diner, he told them the task was hauling drugs, and that it would pay well. At no time was he in danger, because these two were simply out of work truckers seeking to earn some money, not dangerous types. The truckers accepted, and he arranged for them to be stopped and arrested after his men, also undercover, loaded the contraband into the truck. The county attorney refused to prosecute, because this case was entrapment.

There used to be a belief that carrying a gun automatically spelled "cop." Not so. Probably never so. Lawbreakers are often armed, especially in some areas.[1] What is a giveaway is the undercover agent's carrying what's come to be known as a "police special,"[2] a revolver in caliber .38 or .357 Magnum, with a four-inch barrel. Even this isn't absolute. Drug dealers carry weapons for protection, and these are fine revolvers. The reason for drug dealers' commonly being armed is the prospect of a drug "burn," in which the buyer comes to a meeting without the money, but intending to "rip off" the dealer. It works the other way, too, with a person posing as a dealer seeking to rob the buyer of his money.

From this we see that in some cases weapons are not only common, but justifiable. An undercover narc can, through no fault of his own, be on the scene when a "burn" comes down, and may have to fight for his life.

The type of weapon will depend strongly on the locale. In the eastern states, where there tend to be strong gun control laws, concealability is a must. A small revolver or auto pistol will fit this need quite well. In the western states, where gun control laws are lax or absent, almost anything will do. A large Government Model is a popular choice, and the large 9mm auto pistols with double-column magazines are becoming more common. Many people carry carbines or shotguns in their trucks.

The most important quality needed is reliability. The weapon must fire with the first pull of the trigger — no ifs, ands, or buts.

"Stopping power" is much less important. Pistols have more than one round of ammunition loaded. The smallest revolver worth considering has five rounds of .38 Special ammunition in the cylinder, and if these don't stop an opponent, nothing will except a tank or a flame-thrower. The maximum caliber for concealed carry should be .38 Special or 9mm Luger. An exception is the Charter Arms "Bulldog" in .44 Special, which is both compact and light. Recoil is severe, but in a life-threatening crisis, the user won't notice it.

There are very expensive custom handguns, loaded with all sorts of accessories, but they're over-done and unnecessary. They're too expensive, and the extras tacked on can impair reliability. Extended safeties, high-profile sights, and the like tend to catch on clothing.

Avoid the cheapies, especially the low-grade imports. They're poorly-made, and tend to be unreliable. Medium-priced weapons, ranging from about $150 up to $500, are usually best. Some specific weapons that have proven to be reliable and effective are:

The *S&W "Chief's Special,"* caliber .38 Special. With a five-shot cylinder, it's thinner than six-shot revolvers and more concealable. Normally, it comes with a two-inch barrel, but a three-inch version is now available. This model also comes in stainless steel, for less demanding maintenance in damp climates.

The *S&W Model 469.* This is a cut-down version of the Model 459, with a three and one-half inch instead of four-inch barrel, and a couple less in the magazine. Still, twelve rounds of hollow-point 9mm will do the job, and this pistol is compact enough to slip into a pocket. Very reliable.

The *Heckler & Koch P-7.* This import comes in eight and thirteen-shot versions. The one with thirteen rounds has a thicker grip, to accomodate the double-column magazine. Both are unusually reliable, especially with bad ammunition. It's hard to get this pistol to jam. This pistol, at about $500, is the most expensive of the bunch.

The *Walther PP* and *PPK* are good choices, available in both .380 ACP and .32 auto. Both automatics have a fifty-year reputation for reliability, and are worth considering. The PPK is more compact than the PP, but the difference isn't very great. Both are very concealable.

In smaller calibers, the *Raven* and *Bauer auto pistols* in .25 ACP are well-made and reliable. The Raven, especially, is inexpensive at under $100, yet has surprisingly high quality. Both are tiny, and fit almost anywhere, even in a sock. Don't try to run with one of these in your sock, though. It'll surely fall out.

The *ERMA Excam RX-22* is a "sleeper," an unusually good auto pistol in .22 Long Rifle that isn't well-known but is well-made and completely reliable. With a three and one-half inch barrel, it fires the CCI "Stinger" at about 1250 fps, which means good

expansion in the target. It's small, flat, and light, and carries eight rounds in the magazine.

Holsters can cause problems. Usually, a holster is associated with the police. A "pancake" holster, or a "high-rise," almost screams "cop" although these are openly available to civilians.

The best carry is in a pocket. This is less bulky, although less handy, than in a holster. Pocket carry is a very slight advantage in concealment, because holsters are made only for certain spots of the body — the belt, armpit, or ankle — and it's quick and easy to pat down in these areas. No carry is proof against a thorough search, however, and the best protection is to be open about being armed. An explanation of needing the gun for "protection" is acceptable almost anywhere. Open carry in locales where this is customary is a good solution.

Thus, we see that weapons, although rarely essential, are helpful in some situations, and often easily available. Of course, the wearer should be intimately familiar with his weapon, and know how to use it quickly and effectively for best results.

Sources

1. *DEA Narcotics Investigator's Manual*, Paladin Press, Boulder, CO, p. 104.

2. Although Colt makes a revolver known as the "Police Positive," a well-liked police weapon, the gun can be a Smith & Wesson, Ruger, or similar make.

AVOIDING PITFALLS IN UNDERCOVER OPERATIONS

Fictionalized accounts make it seem so easy. The agent infiltrates his targets, faces danger bravely, has a shootout and a car chase, and the story ends with success. In real life, there are some severe problems, and a quick look at them will give you a perspective from which to evaluate the progress of your operation.

Bad Information

One police department staged a raid on a cocaine dealer as a result of a defector, an acquaintance of the dealer's who cut a deal with them, offering to inform in return for special treatment after an arrest. One morning, the police raided the dealer's home, expecting to find him and his stash. They didn't find the stash or the dealer. The information was bad, and they never were able to discover why. Perhaps the dealer had had a last-minute change of plans. Possibly he didn't trust the informer.

The 1984 Olympics

Federal and local agencies went all-out on this one, to assure security and to forestall terrorists. Before any direct security measures went into effect, there

was an effort to penetrate terrorist groups and discover their plans. The result was exaggerated and alarmist "information," some accounts suggesting that terrorists were preparing an all-out assault on the Olympics. Others even pin-pointed some of the "safe houses" that the terrorists were planning to use.[1] As a result, state, federal, and local governments spent over $100 million to safeguard the events. After the events were over, the police congratulated themselves, saying their massive security measures had deterred the terrorists.

Evaluating what really happened isn't as difficult as it might seem. While it's impossible to prove definitely there never was a terrorist threat, or to conclude there was no deterrent effect, some informed guesswork can shed some light on the subject. Deterrence seems a poor explanation. Terrorists have driven truck-bombs into camps filled with combat-ready U.S. Marines, and carried out other attacks against military forces in well-defended positions. It seems unlikely they would fear police SWAT teams. There has been no attack on Olympic games since Munich in 1972, which shows that terrorists don't view the games as suitable targets.

It seems more likely that police over-reacted to bad information, and exaggerations by agents seeking to justify themselves. Part of the explanation also has to do with empire-building. Some police administrators find that releasing "information" of a new and severe threat to the civil higher-ups helps to get them increased funds for their departments.

Empire-building

One state police officer[2] told candidly of his superior's talent in this regard. His superior often ordered him to ghost-write reports to present to the

governor, outlining a new threat to justify an increased appropriation. Drawing upon information from undercover agents, which included defectors, this officer would carefully select the ones that gave the most alarming picture and weave them into a compelling narrative of imminent danger. This tactic was very successful over the years, partly because the empire-building police executive showed good judgement in keeping his claims in proportion, and did not make any claims that could be definitely proved wrong and embarrass him later.

Such techniques are common. They involve avoiding any definite predictions that can rebound when they don't come to pass, and using vague and weaseling language to infer a threat, rather than to define it sharply. Qualifying phrases, such as "may happen soon," "vulnerable to attack," and "capability to strike" are very useful in a report, because it's hard to pin anything down, and the official can avoid having to put up or shut up.

Sometimes bad information is *obviously* bad, but police officials and others accept it credulously and uncritically, and build upon it. One outstanding example was the threat to contaminate the Chicago water supply with LSD during the 1968 Democratic Convention. This caused a furor, and officials took it at face value. A simple calculation would have disclosed that to contaminate the water supply of a city as large as Chicago would require more than the entire world supply of LSD!

What does this mean to you? How can you safeguard yourself against bad information and exaggerations by those seeking to enhance their value to you?

First, do your homework. When something seems unclear, or especially outlandish, question the basic assumptions. In the Chicago incident, officials

assumed the people who said they would insert LSD into the water supply were able to do so, and nobody tried to work out the amount of the drug this would require, and try to discover if there was, in fact, enough of a supply available. A good dose of realism goes a long way toward getting an accurate picture.

Scrutinize carefully your own attitudes and prejudices. The people who make a living at running undercover operations are skilled practical psychologists, and know how to take advantage of peoples' personality quirks. They play upon peoples' fears, and know how to feed their anxieties. Telling a client what he expects to hear is one way of assuring continued employment.

To give a hypothetical but believable example, an employer who fears unionization may fall upon an investigator who, when he finds no evidence of union recruiting, digs deeper. He may tell the employer that the brother-in-law of one of his employees is a union official, or that another employee described what a union gained for him at a previous job. This seems outlandish, but an employer who is so concerned about possible union activity that he takes illegal measures to check it out is ripe for this sort of exploitation. An investigator who tells him he has no cause for concern will be out of a job immediately. One who tells him there is danger is likely to win himself a lucrative contract to keep at it and ferret out other information.

Avoid depending on someone else's conclusions. Try to scrutinize the raw information, rather than accepting "intelligence estimates," and "information received." Be cautious when you see breezy language such as "the smart money says that..." or "intelligence estimates." Phrases such as these often are designed to conceal ignorance rather than reveal knowledge. Going to the source often clears the picture up dramatically.

This can be difficult to do practically, because both police and private agencies are extremely reluctant to disclose precisely who are their informants and agents. However, reading the raw reports, if available, can often show where a possibility got changed to a definite fact in the rewriting.

Compare different sources of information. If you hire a private agency to do undercover work for you, hire another one to duplicate the effort, keeping each ignorant of this redundancy. Compare the reports you get from each, and you'll soon see whether they confirm or contradict each other. Another step is to insert your own undercover agent as a check. You'll have direct access to his information, and be better able to evaluate it.

Finally, use common sense. This means both using your head when evaluating reports and avoiding panic inspired by a threatening or sensational report.

Sources

1. *Disruptive Terrorism*, Victor Santoro, Port Townsend, WA, Loompanics Unlimited, 1984, pp. 65-78.

2. Personal acquaintance of the author, who disclosed the nature of his duties on promise of confidentiality.

CONTROVERSIAL ASPECTS OF UNDERCOVER WORK

There's a very sleazy side to undercover work, involving such practices as entrapment and planting of evidence. These are illegal in this country, unlike in some repressive regimes, but they still happen, and sometimes for the best motives. The chapters that follow will be fascinating, although undocumented. The topics are very emotional, which is one reason for the lack. Much of this information comes from rumors that float around the world of law enforcement and other sources, and agents and their supervisors simply don't put these activities on paper.

We shall see that, not only are these methods not included in reports, but the official paperwork contradicts them. They're mostly illegal, and to prosecute a case, it's not only necessary to avoid tainting the evidence by admitting to illegal means, but the reports must show that the evidence is legally obtained. In other instances, officers and private agents use illegal means that are tangential to the evidence, as we shall see, starting with the first example, blackmail.

BLACKMAIL

Among the unsavory practices associated with undercover work is blackmail. The stereotypical image of career criminals victimizing a respectable person for a past mistake is only part of the picture. Both private and public officials use blackmail, in ways that are both subtle and heavy-handed.

Some Americans are aware that certain foreign espionage agencies use blackmail to coerce officials of other governments to provide them with information. One early example was that of Colonel Alfred Redl of the Austro-Hungarian Army.[1] Redl was a homosexual, and also had expensive tastes. Homosexuality isn't quite accepted today, and usually is a disqualification for government service. At that time, before World War I, it was a criminal offense. The Russian intelligence service somehow found out about Redl's sexual preferences and blackmailed him. They used the carrot and stick approach, though, also paying him large sums of money to enable him to live the high life he craved.

Austrian counter-intelligence agents caught Redl through routine surveillance, watching a suspicious General Delivery package at the post office. They witnessed him picking up this package, which contained a large sum of money. It didn't take long to wrap up the case from there. He never went to trial. Instead, he got an early counterpart of the modern-day practice of "dying of the measles." A group of

army officers visited him and discussed the situation, leaving him with a pistol. Redl committed suicide, because officers and gentlemen at that time were supposed to do "the honorable thing."

Homosexuality, although widespread and almost traditional in certain official agencies such as the British Foreign Office, isn't as well tolerated in the military services, even today. One homosexual who ran into trouble was John Vassal, who inadvertently allowed the Russian KGB to photograph him at a homosexual orgy in Moscow. From that moment, he was theirs. He worked for them, passing them secret documents from the British Admiralty.[2]

In Nazi Germany, the *Sicherheitsdienst* (security service), organized a very exclusive brothel for foreign dignitaries. Although this "Salon Kitty" specialized in "normal" sex, clients were open to blackmail because jealous wives don't take kindly to their husbands' extra-marital activities.[3]

It seems to be normal practice among the larger espionage agencies, with budgets that can afford such extravagances, to employ both males and females for "special services." Diplomats stationed in Moscow, for example, can find attractive Russian citizens who are very friendly and quickly tumble into bed with them. It's hard to clarify how much of this is simply catering to unfulfilled needs, and how much is entrapment. There is no documentation as to who makes the proposition first. The result is the same, and only a few of these espionage targets are exposed.

One was a French ambassador who cheated on his wife with an attractive Russian young lady, but the KGB handled the case in a clumsy manner and the effort came to light after the ambassador's return to France. There was a stormy scene in President de Gaulle's office.

Entrapment is not the only way to acquire blackmail evidence. Other, technical means such as wiretapping serve well.

Let's also not make the mistake of thinking that blackmail, sexual and otherwise, is the exclusive province of dirty, sneaky foreign agents, and that clean-living, clean-cut Americans would never stoop to such measures. One American organization that does this is a large corporation we all distrust and hate — the phone company. One telephone company executive testified that wiretap information was useful when putting pressure on public officials for rate increases. Among the information that telephone company tappers extracted from intercepted conversations was whether or not the targeted official had financial difficulties, or was carrying on an illicit affair.[4]

The telephone company also uses the carrot-and-stick approach that works well for espionage agencies. A city councilman with financial difficulties could often be persuaded by throwing a little business his way, as well as strong-armed by a telephone company negotiator making an oblique reference to his illicit affair.

There have been other attempts at blackmail which have come to light. At the time Ralph Nader was stirring up the muck against Detroit automobile manufacturers, private investigators were digging into his private life to try to find something which could be used as leverage to shut him up.

We don't know how widespread blackmail is among private investigators. The few examples which have come to light are surely only the tip of the iceberg. Political campaigns are often very dirty, with candidates employing private investigators to dig up any dirt about their opponents. The Hollywood film *The Best Man* was a fictionalized version of this

practice. Most of the real-life counterparts remain unseen, because victims usually give in rather than expose the blackmailers and themselves.

There have been documented examples of government-run blackmail brothels. So far, there has been no privately-run one exposed. Perhaps one of these days there will come out a case of an enterprising private investigator setting up a brothel to gather information generally, in a "fishing expedition." Scanning his list of "clients," he can determine which names are likely to be profitable, and seek out the person's political enemies to sell them the information.

Thus, we see that blackmail isn't necessarily for personal profit. While career criminals who come across or create damaging evidence do it to extract money from the victim, corporations and government agencies use blackmail for other reasons.

This has had an effect on recruiting practices and security screening. Security officers, when they investigate applicants, take an interest in possible subversive connections, and also a shady past that might open up the subject of blackmail. They watch for continuing tendencies such as homosexuality — not for reasons of prudery but because they know from experience that this can be exploited to put irresistable pressure on a targeted individual.

Among the more enlightened agencies, such as the CIA, there's a viewpoint that many people have shameful incidents and backgrounds, and that it's best to face it and deal with it than to leave it unresolved. An employer who knows about an unsavory fact in an employee's life and doesn't use it as a disqualification can actually protect his employee from blackmail. The victim knows that this fact can't be used to ruin his career, and this makes him less vulnerable.

Employees in sensitive positions receive security briefings, during which they're warned about possible attempts to blackmail them, and the means by which blackmailers can entrap them. They're warned, for example, about sexual liaisons in foreign countries. Security officers emphasize that if there is a blackmail attempt, they should immediately report it, no matter how damaging the information might be. In the enlightened agencies, policy is that the blackmailed employee will receive special consideration if he reports the incident to his superiors. They go easy on him because it's less damaging overall to confess immediately than to comply with the blackmailer's wish to start a career of betrayal.

Sources

1. *Spies & Spymasters*, Jock Haswell, London, Thames & Hudson, 1977, pp. 107-108.

2. *The Making of a Spy*, Raymond Palmer, Crescent Books, 1977, pp. 84-85.

3. *Spies & Spymasters*, p. 141.

4. *The Private Sector*, George O'Toole, New York, W.W. Norton Company, 1978, p. 70.

ENTRAPMENT:
A POST-GRADUATE COURSE

We've already seen that entrapment is not allowed, as it taints the evidence. The judicial rules are quite strict and explicit about how far the undercover officer or private agent can go in dealing with a suspect. Nevertheless, entrapment occurs. Very little of it is documented, for obvious reasons. There are basically two ways to entrap a suspect.

The first is for the officer to make the solicitation himself, and then offer perjured testimony in court. This way is simple, and saves a lot of time in an undercover investigation. It's very hard for a suspect to prove he was entrapped when the case comes to trial. Usually, it's his word against the officer's, and the court usually accepts the officer's version.

The second way is indirect, and amazingly enough, is documented in a book by a retired U.S. Secret Service Agent.[1] This method has the undercover agent working in tandem with an informer. The agent never makes any solicitation, because he knows he must be prepared to testify truthfully to what he did and said.

Instead, the informer sets the scene, telling the suspect beforehand that the agent is seeking drugs or other contraband, or is willing to participate in the crime. This prepares the agent to come on stage quite innocently, and accept the solicitation offered by the suspect.

Entrapment is a short-cut, and it sometimes backfires. If it does, the result can be a large lawsuit, and even criminal prosecution. However, there's no way of knowing how many instances of entrapment go well for the agent, helping him to perfect his technique and encouraging him to do it again at the next opportunity.

Entrapment is a classic secret-police technique. Government agents who infiltrate political groups often suggest they do something illegal, exposing them to prosecution. The reason this is common, is the method of "working" the case. This involves "setting up" the target individual or group, and can also apply to non-political cases. The infiltrator is actually an agent-provocater, who suggests that the group do something illegal, such as robbing a bank or committing sabotage. This is entrapment to a higher power. He helps in the planning, and may even go along with the execution. Of course, he's kept his control informed, and when the deed comes down, the police are waiting. If the group has tight security, the agent must be arrested along with the rest of them, to avoid suspicion. Later, the police can arrange for the agent to "escape," so that he can continue his work.

An extraordinary case of an agent-provocater that came to light was that of Ievno Azeff.[2] This man was an agent of the Ochrana, the Czarist Russian secret police. He not only worked as an agent-provocater, but engineered the murder of his boss.

Having started out in life as a common criminal, he fled Russia to Germany, and after awhile offered his services to the Ochrana as an infiltrator of rebel Russian expatriate groups. He posed as a revolutionary, meanwhile collecting names and reporting the activities of the groups to his masters in the Ochrana.

Apparently he had much success, and was well-accepted by these groups. He returned to Russia to infiltrate the local terrorist groups, posing as an ardent activist. Among the feats he carried out was the assassination of the Grand Duke Sergei. In 1905, he participated in the fatal bombing of Plehve, the Czarist Minister of the Interior who was over the Ochrana. In one sense, this assassination was a result of the Byzantine politics of the Czarist government, because Azeff's control was in on the plot, and could have prevented it. The reason he didn't was a classical case of empire-building, as he wished to demonstrate the need for his department, and obtain increased appropriations.

This case served as a prototype for others. An ambitious secret police chief, seeking more power and recognition, is never going to make it if there's no demonstrable threat. A sleepy, peaceful political opposition isn't a credible threat and doesn't justify a massive investigation. It helps to have a few bombings and killings.

One way to arrange this is to infiltrate undercover agent-provocaters. Their role is clearly not to gather evidence, but to make things happen. Even if the movement is peaceful, the agents can start an "activist" faction, oriented toward violence. In any group, there are always a few hotheads, impatient with the slow pace of progress, and who can be re-directed towards more direct action.

This is one of the safest undercover activities, because the agent-provocater never has to break his cover to give evidence in court. He never has to take risks to gather evidence. His function is merely to incite, and to pass on the information to his control. For these reasons, such an agent is rarely exposed.

The same pattern applies in private investigation. It helps to "build up" the importance of a case. An ambitious security chief can fake an incident. One of

the possibilities is to plant a bomb, one that doesn't do much damage but that highlights a "terrorist" threat. The corporate executives, alarmed by this event, will more readily give him the means to increase his department's size and importance. Engineering such an event requires some fine judgement, because it can also backfire. The top management may conclude that the outrage occurred because of the security director's incompetence, and replace him.

In the public sector, one such incident that came to light, to the embarrassment of the Los Angeles Police Department, was at the 1984 Olympics. After a long build-up of security measures, with copious publicity, the Olympic Games seemed anti-climatic. SWAT teams were deployed, ready to cope with terrorist attacks, but nothing happened. The only noteworthy violent event was that of a motorist, a psycho, running down people by driving on the sidewalk, something unconnected with the games themselves. The ambitious police officer who planted the fake bomb sought to gain recognition, but was quickly discovered.

There's no way of knowing how many instances of provocation have happened, because this is the most deeply-covered clandestine activity of all. Much depends on the ambition and ethics of the secret police chief, or the owner of the private investigative agency. As we've seen, some of them have no ethics at all.

Sources

1. *Undercover*, Carmine J. Motto, Springfield, IL, Charles C. Thomas, Publisher, 1971, p. 82.

2. *Spies and Spymasters*, Jock Howell, London, Thames and Hudson, 1977, pp. 106-107.

INDUSTRIAL ESPIONAGE

Seeking out information on a competitor's materials, products, and trade secrets can produce profitable results. Normally, "everybody does it." Usually, it's by perfectly legal means.

It's not a crime to read a competitor's advertisements, to attend trade shows and inspect his products, or to ask his customers how satisfied they are with his products or services. This is normal industrial intelligence and many large and small companies do it. Some have special departments for this, and don't bother to hide them.[1]

It's easy and legal to buy a few shares of a competitor's stock, in order to be on the distribution list of his stockholders' reports and to attend stockholders' meetings. Reading the business section of the newspaper is another way of gathering open intelligence about a competitor. So is buying a sample of his product and analyzing it. Sometimes, however, the intelligence-gathering crosses a hazy line to unethical and even illegal practice.

Hiring away a competitor's help is one way of getting the "inside story." The one who does it calls it "aggressive recruiting," while the victim calls it "pirating." It all depends on your point of view.

Sometimes, the hiring away can be for the express purpose of wrecking the competitor.[2]

Going further, there are spurious job offers, placed by dummy corporations or even real ones, aimed at interviewing the competitor's employees. The offer can be made to seem generous enough to attract attention, and once the employee is in the interview, it's easy to ask him about his current job in great detail, in the guise of probing his qualifications. This is an old trick, but it sometimes still works.

Many employees are sophisticated enough not to fall for this. Others are constrained by secrecy agreements, non-disclosure clauses in their contracts. The employer obliges a new hire to sign a statement that he will not disclose sensitive processes while he's employed, or for a specified number of years after he leaves. These agreements have held up in court, and there have been lawsuits for breaking them.

This sort of agreement applies even to the employee who breaks off to start his own business. Breaking off from the "parent" company is common, and many new companies have started this way.

Light Cover

Another way to obtain a competitor's high-tech secrets is to pose as a potential buyer. One way to do this is through a dummy company, but this is shallow and can't stand up to even a superficial investigation. A better way, one that involves no conflict of interest, is through the "old boy" network. An executive who wants information about a competitor can make use of a friend or old school chum working for another company that is or might be a customer of the competitor's. In that position, the friend can ask about the technical specifications of a forthcoming piece of equipment, and might even get them if he's highly regarded. Simply keeping his eyes and ears open can do wonders.

Typically, customers receive invitations to visit the plant, and get guided tours which can last all day. This provides an important opportunity for a highly-trained technician or engineer to winnow out industrial secrets. A small detail that would tell a layman nothing can be very revealing to the trained eye.

There can be payment for this sort of informal arrangement, and the transfer of money isn't always compromising. It doesn't have to be in cash. Gifts of material goods, paid vacations at company expense, and country club memberships are all ways of arranging this discreetly.

Infiltration

This means placing an undercover agent into the competitor's organization. This can be very difficult, because unlike infiltration into a company by invitation, there's nobody to help, and there surely will be security measures to keep infiltrators out. An employee can apply at the competitor's company, where he might be received one of two ways. He might be seen as a potential source of information, milked thoroughly while being kept at arm's length from any proprietary information, or he might be refused outright. A safer way is to recruit someone who is not an employee, through conventional channels. Classified ads for the same position that the competitor has open will attract the same group. The most likely one can be the subject of the proposition: "Take the job with them, but work for us."

The problem with this approach is finding the person who is both willing to do it and most likely to be hired. They don't often coincide. If they do, and the plan succeeds, the normal undercover rules

apply. There are two paychecks, methods of secret communication, etc.

Getting an infiltrator or agent into place is chancy. It's much easier if he's already there.

Suborning

Suborning a competitor's employee is simple, but can become very involved. Basically, it's trying to recruit a defector. It's true that an employee who "comes over" can reveal a lot about the competitor's processes and trade secrets, but his change of employment is in the open, and his former employer will be watching carefully to detect any breach of security. Also, his information dates from the day he leaves, and becomes progressively obsolete.

Keeping him as a defector-in-place is more rewarding for both parties. The employee continues to collect his paycheck, and now has another source of income. This can be an embarrassment if he's not discreet, and can be proof that will stand up in court if there's ever a prosecution. One way of avoiding this is for the company doing the espionage to form a dummy company and hire him as a "consultant," an old dodge that works very well. Keeping everything "on the books" avoids complications with the Internal Revenue Service, and provides a plausible explanation if the defector decides to do some high living.

If the defector's level-headed and discreet, he can ask to have the money deposited in a foreign account, as a nest-egg for retirement. Alternately, he can have one of his family hired by the dummy company, as a cover for the income. There are all sorts of permutations of payment that can arrange the transfer of money without detection or arousing suspicion.

Illegal Means

Breaking and entering is not common, but does occur. This is very direct, and apart from the prospect of getting caught, lets the competitor know that someone's after his secrets. While it doesn't take much sophistication to try to camouflage the break-in as an ordinary burglary for profit, it takes no great intellect to see through this trick, either.

Modern industrial plants have many concentric layers of security. There are perimeter fences, guard patrols, door locks, door and window alarms, infra-red, sonic, and capacitance sensors, and finally, sophisticated safes for vital documents. None of these is impenetrable, but together they're powerful deterrents. This is why B & E is far less common than legal means of stealing industrial secrets.

Sources

1. *The Private Sector*, George O'Toole, New York, W.W. Norton Company, 1978, pp. 50-52.

2. Several years ago the author worked as a technician in a small shop that had only two large accounts. The author, at that moment, was the only technician, and the accounts needed daily servicing. A phone call from a competitor resulted in a job offer. The author explained that his leaving at such a critical moment would paralyze his employer, losing him his accounts, but this didn't seem to bother the person trying to hire him away. It wasn't hard to calculate the real purpose behind the job offer, and was even possible to guess how long the new job would have lasted once the former employer was out of business.

METHODS OF PAYMENT

Paying informers has its drawbacks, as we've noted. Sometimes it's necessary. In certain instances, there's an active program to pay informers because this is one way to get responses and other choices are very unproductive.

One such program is the "turn in a friend" operation used by the Internal Revenue Service. This involves paying up to ten percent of the taxes recovered to a snitch who informs the IRS of a case of tax evasion. As the IRS keeps this activity's success, or lack thereof, a deep secret, there's no way of evaluating how useful it really is.

Another "informing for pay" program is one run jointly by the Federal Drug Enforcement Administration and local police agency narcotic squads. The DEA fronts the money, and the local agency does the donkey work.

The first step is to place ads in newspapers, offering up to five hundred dollars for information leading to the arrest of a drug producer or dealer. The offer includes a promise of confidentiality. The ad gives an 800 number to call, which is manned twenty-four hours a day.

The police, when they get a call, don't ask for the informer's identity. They assign him a number, and instruct him to call back, giving that identifying number, in a couple of weeks, after they've had the time to follow up on the lead.

If the lead is valid, the police determine the amount of payment, and when the informer calls again, they decide on a method of delivery. If the caller wishes, a police agent will meet him and hand over the money when he identifies himself with his number, and will not seek to follow him or discover his identity.

In the case of a very suspicious caller, the police will even consent to leaving the money at a "dead drop," where the informer may pick it up after the police agent has left. The police "play it straight," knowing if they betray the trust, the news will get around and compromise the whole program.

It often happens that the informer's motivation is not only profit. The caller may be a drug trafficker himself, using the police to eliminate a troublesome competitor. This is the irony. The police, by acting on the information received, make an arrest and thereby increase the trade of another trafficker, meanwhile paying him in cash for his information.

Another irony is that this anonymous cash payment enables the informer to avoid paying the income tax due on it. The informer gains because the IRS turns a blind eye to this practice.

How effective is this sort of program, whatever the moral issues? The police don't publish their track records regarding informer programs, but the available information, based on off-the-record statements by police officers, direct observation of the results gleaned from some such information, and the overt evidence of the increasing drug trafficking in this country, suggests that the results are poor.[1]

The reality is that police narco units spend a lot of man-hours following up bad leads. Of course, a bad lead results in no payment, but the police do spend the man-hours. It's hard to imagine a less risky way of wasting the time of the narco units than phoning

in bad leads and sending them on wild goose chases. With an 800 number, the caller doesn't even pay for the call!

One state police force has an aerial reconnaissance program for spotting marijuana from light planes and helicopters. A highly-trained narco agent and a pilot fly from six to eight hours a day during the growing season to try to spot "gardens" of marijuana plants. The agent, reading from "tips" in a small notebook, directs the pilot to various sites for a close observation. This activity is mostly unproductive, because in three years, this agent has spotted only 28 gardens from the air. One obvious conclusion is that growers phone in "tips" to keep the agents busy chasing ghosts while they continue to grow their plants undisturbed elsewhere.

It isn't surprising that the police often find themselves second best in the game of wits. They sometimes say that criminals are dumb, but the great number of crimes and the low rate of clearance suggest otherwise.[2]

It doesn't take much imagination for a drug dealer to gather information about a competitor and phone it in. Even one without an extraordinary intellect may think of "planting" evidence that the police will find. The police, acting on the information in good faith, find the evidence and make what they see as a valid arrest, never realizing that the affair was a "set-up."

A very controversial and strictly sub rosa method of payment is in drugs. Police sometimes hold back drugs from seized evidence, and divert it to supplying some informers. This is an outgrowth of "walking around money" that the police often pay to their informers.

Strictly speaking, this is not a reward, but a maintenance payment. The informer incurs expenses, and may not be able to meet them out of

his own pocket. If he's an addict, maintaining him is a logical way to keep him functioning and producing information. The police detective doles out enough to him to feed his habit, but not enough to enable him to deal, unless this is a requirement of the case.

Sources

1. *Undercover*, Carmine J. Motto, Springfield, IL, Charles C. Thomas, Publisher, 1971, p. vii. The author, retired U.S. Secret Service Agent, states that a 30% or 35% success rate in undercover operations would be an exceptional performance. Although he refers to counterfeiting, this figure can apply to other types of undercover work. It's almost certain that the figure would be much lower in other instances. Counterfeiting and the theft of securities involve documents, pieces of paper which the criminal must convert into cash. Thus, he has to come out into the open, even if only momentarily. Drug trafficking is all clandestine, and for this reason much harder to trace. Speculating on the success rate of narcotics enforcement officers can't be more than guesswork, but the probability is that the percentage is appallingly low.

2. *Uniform Crime Reports*, Federal Bureau of Investigation, Washington, DC, U.S. Government Printing Office, any year. An almost-forgotten study popularized in a national news magazine at least two decades ago showed the results of I.Q. testing among a sample of penitentiary inmates. The average I.Q. was 83, dull-normal and almost down to the moron level. The study purported to "prove" that criminals are stupid, but in fact it didn't. What it proved was the mental level of criminals who were caught by the police and successfully prosecuted through the leaky, creaky criminal justice system. We can speculate about the intelligence of those who don't get caught.

PLANTING EVIDENCE

Years ago, a newspaper reporter in a college town that was experiencing some peace activism during the Vietnam War era was offered a five-dollar "baggie" of marijuana under strange conditions. He was visiting the local Salvation Army office, where the office manager, new in the post, was to supply information about a food drive he wished to publicize. The manager pulled a baggie out of his desk and told the reporter that it had been given to him by a man the reporter had met during the course of his work, and who was allegedly an avid fan of the reporter's. The baggie was supposed to be a token of his esteem for the quality of the reporter's photographs.

The story sounded strange. The reporter was suspicious. He knew the office manager had told him that he had recently come from Guam, where he'd been stationed as a civilian employee of the U.S. Army, and had assumed the job with no previous experience in the field of social work.

This was the era when local and Federal agencies were infiltrating the "peace" movement, and the reporter, although he was not part of it, had many contacts within the local peace movement. He suspected he was being "set up," and that if he accepted the marijuana, he might well be arrested after leaving the office and coerced into providing information in return for the dropping of charges.

This reporter did not normally smoke marijuana, and really didn't want it. He flushed the contents of the baggie down the toilet in the manager's presence, and walked away from the encounter. Within a year, the manager disappeared as suddenly as he'd arrived, confirming the reporter's suspicion that he was an undercover agent-provocater.[1]

Planting evidence is perhaps not as common as it was years ago, but it's an effective method to cultivate an arrest or to get a "twist" on a potential informer. In human terms, it's easy to understand a police officer, exasperated by a suspect whom he "knows" is guilty, deciding to help his case along by planting evidence.

In the police subculture, there's a widespread belief that the law, the courts, and the rest of the criminal justice system are designed expressly to frustrate police officers in their efforts to neutralize criminals. Police tend to be impatient with the legal safeguards provided by the U.S. Constitution, because they see that, although the small offender is relatively easy to prosecute, the sophisticated big-time operator knows every loophole the laws allows, and has an attorney who takes full advantage of them.

In this light, police investigators are often tempted to take short-cuts, to tamper slightly with the evidence, to make a case. This remodeling may be as mild as perjury to establish "probable cause," or it may be an outright planting of evidence.

In criminal cases, there may be more than one reason to plant evidence. The obvious one is to be able to "bust" a suspect for possession of contraband, or to be able to provide evidence of guilt on a specific charge.

The second is to hamper the suspect's activities. Some states have laws that stipulate that police may

confiscate any goods or instruments used in a crime. In the case of illegal substances, such as drugs, the connection is obvious and clear, and affords the police their best opportunities.

A police officer who finds drugs in a car can make a case that leads to confiscation of that car. An aircraft used in drug smuggling is also liable to confiscation, if an officer finds drugs in it, no matter what the quantity. Taking a drug dealer's car or airplane imposes a hardship on him, and puts a kink in his operations, as well as giving an open window to a criminal prosecution.

What happens to the confiscated items is the most interesting aspect. Many under-budgeted enforcement units welcome the acquisition of a car or airplane to help them in their efforts. A car can be useful for shadowing, especially if it's a different make and body style than the unit's vehicles. Many narco detectives and undercover agents make good use of confiscated vehicles. An aircraft is useful for spotting marijuana fields from the air, and in fact several narco units use confiscated aircraft for this, as well as some procured through the normal budget.[2]

Money and drugs seized are useful for subsidizing undercover operations. They serve to pay informers, who collect both in money and in drugs. Although not legal, officers sometimes make subsistence payments in drugs. In other instances, they can use a seized supply of drugs to make a "sale."

Under some state laws, outgrowths of the Federal "RICO" (Racketeering Influenced and Corrupt Organizations) law, the proceeds of crime are subject to confiscation, to take the profit out of crime. When law officers can apply this, it's very effective and can cripple an illegal operation, leaving the defendant without enough funds to pay for a lawyer.

Planting evidence is useful in private investigations, too. While it's illegal to investigate union activities, a private agent can work for the ostensible purpose of uncovering a theft ring, substantiating his operation by planted evidence. A company president who fears unionization can hire an undercover agent to plant evidence of theft among the union organizers. This gives good "cover" for an investigation resulting in dismissal of the employees, and even prosecution.

None of this goes down on paper, of course, to prevent any legal complications later. Thus, we see that an undercover operation can run on several levels, have wheels within wheels, one layer concealing the ones beneath.

Planting of evidence isn't limited to law officers or company officials. Members of a theft ring may plant evidence on an innocent party to draw suspicion away from themselves. There may not even be any criminal activity. In company politics, there's often sharp rivalry between upward strivers angling for favor or promotion. Planting evidence is a way of discrediting a competitor. This technique can have many subtle variations.

A machinist, his eye on the foreman's job, may slip a defective piece or two into a bin of parts turned out by a rival for that job. Leaving the classified section of a newspaper open to the employment ads on a rival's desk for others to see can "incriminate" him indirectly, suggesting that he's job-seeking.

We see that there are endless possibilities of abuses in undercover work, many ways of circumventing the law effectively to gain an advantage and to fabricate a case. Because a cover-up is an essential part of such an effort, there's no way to estimate accurately how widespread these illegal practices are. Using the "tip of the iceberg" theory, we can assume that, for every one exposed, there are many that remain deeply in the shadows.

Sources

1. Personal knowledge of the author. This example, with its uncertainties and guesswork, illustrates perfectly the shadowy world of undercover work.

2. A member of a sheriff's department revealed quite candidly that he and some others on the staff were quite eager to procure an aircraft or two for the department, as they had in the past. Previous aircraft had been confiscated from drug smugglers, and served the sheriff's department well for aerial surveillance. Some time after this discussion, the sheriff's department was involved in two unsavory affairs dealing with planted evidence and entrapment, but it still hasn't managed to seize an aircraft.

BOWING OUT:

TERMINATION OF THE ASSIGNMENT

Once the case is closed, what to do with the agent becomes a question that needs a shrewd answer. In certain instances, it answers itself. The undercover agent who testifies in court blows his cover. This happens in cases where prosecution is more important than retaining the agent in place.

Where there's no imperative to expose the agent, it may be advisable to keep him running. In an employment misconduct investigation, the agent doesn't necessarily suffer exposure, and it's almost certain that there will be more cases to investigate in the future. A bonus is that the longer the agent stays, working discreetly, the deeper and more impenetrable his cover becomes.

In some instances, the agent terminates himself through stupidity and clumsiness. As discussed in the chapter, "Getting Down to Cases," the undercover agent who told the boss that he'd have his resignation after the union election blew his cover, if he had any left, right then. This agent was clumsy and emotionally unstable, trying to lead a life that conformed with his adventurous and conspiratorial fantasies.

A sudden departure at the conclusion of the assignment can only lead to suspicion. This doesn't affect the current case, but if there's any future need to insert an undercover agent, it will be more difficult.

The agent who stays in place can report on the after-shocks of the dismissals or arrests. He can also try to uncover any persons who were not detected in the first phase of the investigation. Sometimes, disposing of a criminal ring creates a vacuum, and someone else steps in to fill it. These are good reasons for trying to keep the agent in place after the immediate assignment is over. Some companies have permanent undercover agents as a matter of course, just as some government intelligence services maintain "sleeper agents" who don't do anything until activated. Keeping an undercover agent as a "sleeper" can be expensive, but in the long run, it facilitates quick reaction if a problem comes up.

The sleeper protects his security by being inactive. During this phase, which can last for years, he makes no contact, conducts no investigation, and doesn't risk exposing himself.

Activating a sleeper can come about in two ways: the control can contact him with new instructions; or he can activate himself if he comes across something which deserves attention. In such a case, there's a pre-established method of contacting the control to explain the situation to him and receive instructions.

In some instances, extreme measures become necessary to protect the agent's usefulness. Carmine Motto, an undercover Secret Service Agent, was "arrested" along with others to protect his cover.[1]

Engineering an "arrest" involves long-term planning. The agent may have to spend time in jail, awaiting trial or the opportunity for a rigged "escape." Trial and conviction, resulting in a prison sentence, can cement the agent's relations with his criminal associates, by utterly dissolving suspicion, but few people are willing to spend years in prison

for what's basically just a job. That is why this method isn't practical to carry to its logical conclusion.

If it's necessary to withdraw the agent, timing and method are important. In any situation, the agent can leave for "family" reasons, such as a death or sickness of a distant relative. Meeting or reconciliation with an ex-wife or old girl-friend can be a useful cover motive. He can even arrange to be "fired" or "laid-off" to explain his departure. A new "job" far away also serves to smooth his leaving.

The need for finesse doesn't end with the assignment. Bowing out gracefully is important, both to protect the agent and future prospects.

Sources

1. *Undercover*, Carmine Motto, Springfield, IL, Charles C. Thomas, Publisher, 1971. The frontispiece shows Mr. Motto, looking seedy and disreputable, in a photograph taken by police at his arrest.

DEFENSIVE MEASURES

Because of the widespread illegal use of undercover techniques, it's necessary to cover ways of defense, to give a potential victim the means of avoiding entrapment, "framing," and other dangers. You may feel you lead an honest and straightforward life, and therefore are immune to such nefarious practices. Not necessarily. We've seen some examples of how people innocent of any crime may be victimized to serve someone's purpose. Let's run over a few examples of how and why you might be vulnerable:

■ You might become a suspect in a criminal investigation, although completely innocent.[1] Anyone who works for another can't be certain that all his fellow employees are as honest as he is. If there's some illegal practice where you work, you can be sure of becoming a possible suspect, unless and until an investigation clears you.

■ Watergate. This conspicuous example of double-dealing in politics serves as a warning to anyone seeking political office. While the degree of guilt or involvement of some of the participants is still open in some people's minds, there's no doubt that some illegal methods came into play, including burglary and bugging.

■ Framing by a criminal, to misdirect attention, or to eliminate you as a rival.

■ Industrial espionage. If you're an executive for a large or small company, you know the opportunities for profit inherent in stealing another's proprietary processes. If a rival firm can discover the technical details of a new process or invention before the inventor can patent it, it saves the cost of independent research. Similarly, automobile and fashion designers are always itching to find out what their competitors are doing, and routinely employ agents for this purpose.

■ Blackmail. If you have something you want to keep quiet, this makes you a potential target for a blackmailer. There's every reason to assume that blackmail is much more common than the record of official prosecutions shows. Victims have great incentive not to report the attempt to the police, and to comply with the blackmailer's demands.

■ Union activities. Espionage and undercover work are on both sides of this explosive issue. Companies use spies, and unions often use similar methods to gain an advantage. If you work for a company being organized by a union, or with one already present, you'll find it hard not to get caught in the middle. You'll find yourself being tested by both sides, to discover where your loyalty lies.

■ An "inside man" for a burglary or robbery ring. If you're in a line of business in which there are items worth stealing, such as furs, drugs, electronic equipment and jewelry, you may have an applicant who is really an "inside man" for a criminal gang. His real job will be to "case" the layout, and report back to his accomplices. He'll be looking carefully at your doors, windows, alarm systems, safes, and schedules. Such an "inside man" is virtually undetectable.

Defensive Measures

Let's start out by stating the obvious: there are no 100% effective defenses against undercover

penetration, and the effort involved sooner or later passes the point of diminishing returns. There are various means to reduce the threat, but no absolute barriers. The best course is to take some defensive steps, in order not to make it too easy for an undercover agent. Going to an extreme can take up all your time, have you suspecting all your friends, associates, and employees, and significantly impair your other activities.

The level of your defenses will depend on who you are and what your situation is. You'll want to be more careful if you see yourself vulnerable, or if someone might have an incentive to use undercover techniques against you. If you're in one of the situations listed above, you have reason to be fearful.

Defense against undercover penetration revolves around security techniques, some of which are simple, and others which may be too elaborate and costly to you. Some may even be unnecessary. Let's examine them one by one, and see how applicable they are to you.

Need to know. This is one of the simplest to use, and costs nothing. Don't disclose sensitive information to anyone who doesn't need to know it. One point to watch here is "bar talk," as there are many secrets revealed under alcoholic lubrication.

It's possible to go to extremes in this. An attitude of overt secretiveness will offend associates and employees. It's possible to deflect indiscreet questions without offending, and simply not bringing up sensitive topics will do the rest.

A technique allied to need to know is *compartmentalization of information.* There's usually no need to spread sensitive information throughout the whole group. A company project may be broken up into fragments, all assigned to different departments, with only one or two at the top knowing the full extent of the project and its

progress. Limiting vital information to the few who need to know keeps it in bounds, and if there's a leak you have a ready-made suspect list.

Compartmentalization helps both in limiting damage from leaks and espionage, and in pinpointing the source if it occurs. A piece of information will be known only to a few in the organization, and these will be the ones to investigate if there's evidence that this piece of information has leaked.

A further counter-intelligence technique is "feeding" information to a suspect and watching for results. An example is to tell one suspect that there will be a meeting at a certain time at a certain place, and then watch for surveillance or other reaction. If there is, the leak could have come only from the person to whom you gave this information.

Counter-surveillance. This can work with "feeding." Tailing or shadowing a suspect to see whom he meets can consume a lot of time, but if you limit the surveillance to the period immediately after passing him a morsel of "hot" information, you may see him making a contact.

This is a one-sided technique, because while positive information, e.g., catching him making a suspicious contact, is conclusive, negative information is not. If your suspect is a fellow union member, and you pass him some "hot" information, you may be able to follow him while he goes to the company president's house to deliver it. More likely, though, he'll make a phone call, and unless you happen to tap the phone he uses for this, you won't intercept the call. Negative evidence doesn't prove him innocent.

Background checks on new employees. This doesn't have to be elaborate, but it's important not to accept anyone at face value. A basic step is to check if

the applicant really worked where he says he did. Often, it's possible to check references because you know someone who works at or owns the company at which the candidate claims to have worked.

Often, because in a certain field everybody knows everyone else, it's possible to get "the word" on a new employee simply by asking around. A spurious applicant will stand out.

A history of job-hopping, or a history that doesn't go back by more than a few months in your locale is cause for suspicion. Look very carefully for previous employment in a company that has had labor problems, theft, and other disturbances. This is an early warning that the new man may be a penetration agent. Anyone from out-of-town deserves special study.

Be careful of new acquaintances. This doesn't mean treating them all with deep suspicion, but holding them at arm's length until you're satisfied they're trustworthy. Be especially careful of one who makes damaging admissions, and seems to be using the techniques of "roping," which are subtle.

In this regard, learn to be a sympathetic listener, rather than a talker. Many of us like to talk, and if we must, it's better to talk about a harmless topic such as sports or philosophy rather than a personal one.

Just because someone's been accepted by a friend of yours doesn't mean he's trustworthy. Wait and exercise your independent judgement.

Make it a habit to remain alert, not overtly so, but aware of what's going on around you. Learn people's habit patterns, and scrutinize behavior that departs from the norm.

Watch your property, without making it obvious. Lock your car, and learn to look to see if anything has been disturbed when coming back to your office or home. Remember the way you leave things, and note

if anything's been moved. Use bits of dust or cigarette ashes to determine if anyone's opened your toolbox or briefcase. A staple or paperclip will tell a tale if it's not in the place you left it.

Be careful when drinking. Choose your drinking partners carefully, and never get so drunk that you talk a blue streak.

If anyone propositions you to do something illegal or unethical, be doubly careful. This is especially true if you're involved with a quasi-political activity, such as a mass movement or labor union. There are agent-provocaters out there, trying to lead people into exposing themselves to prosecution.

This can be a double-edged danger. Agreeing to do something illegal can be damaging. Failure to report the attempt can also count against you. Some companies run this sort of "loyalty test" on their employees, and most of the sensitive government services do. One defense against this is to leave immediately whenever you find someone starting to proposition you this way. Don't let your curiosity overwhelm you. If you don't hear the entire "offer," you can later protect yourself by saying that you didn't take the person seriously, or that you thought he'd had too much to drink, etc. Another countermeasure is to laugh, adopting a mocking manner. Remember that the conversation might be taped, and your manner and words will count against you if you listen seriously and take part in the discussion.

If you become aware of someone doing anything dishonest, play it very cool. Don't let him know that you know, if possible, and don't join him, no matter how tempting.

In a new workplace, keep your cards very close to your vest until you know who's who. An indiscreet remark could easily come back to haunt you. A sympathetic person might be the boss's brother-in-

law. Until you've been there awhile, you won't know who the boss's snitch is. In normal times, the "company men" are conspicuous. During management-labor crises, new people may be undercover agents.

Be especially careful in emotional moments. It's very easy, on the job, to say something indiscreet during a moment of anger or frustration. It's also important to keep a low profile during group discussions, when many people feel inclined to speak up. The topic might be dangerous, and keeping silent or non-committal is one way of avoid gratuitous trouble.

Trust your family before you trust outsiders. This is the principle that made the Mafia great. Blood is still thicker than water, in this turbulent century, and family members are less likely to betray you than non-relatives.

Many "family businesses" operate this way, with the key slots reserved for relatives, even though "nepotism" is a bad word nowadays.

Long-term friends are usually more reliable than new ones, no matter how close the new relationship may be. It takes time to infiltrate a penetration agent, or to develop an informer, and one who was a close friend or associate well before the immediate situation is much more likely to be reliable than another who just blew in.

If you're an employer, keep in mind that *the way you treat your people will have a lot to do with their loyalty.* Being fair isn't protection against the professional criminal, but if morale is high, employee loyalty will be high too, and you're likely to have fewer theft and labor problems.

Sources

1. At age 19, while working in a retail camera shop, the author was wrongly accused of stealing a camera by the owner, who forgot that he had sold the camera in question two days before.